

# CMS

Illinois Department of  
Central Management Services



State of Illinois

Public Key Infrastructure

Certification Practices Statement

For Digital Signature

And Encryption Applications Version 3.1

(IETF RFC 3647 format)

March 17, 2009

## DOCUMENT VERSION CONTROL

VERSION	DATE	AUTHOR(S)	DESCRIPTION	REASON FOR CHANGE
2.0	12-Sep-2006	Anderson	Initial draft	Conversion to RFC2527.
2.0	15-Feb-2007	Anderson	Update	Conversion to RFC2527.
2.0	31-May-2007	Anderson, Miller	Update references	Conversion to RFC2527.
2.0	6-12-2007	Anderson	Removed highlighting, accepted changes.	Notified of email approval by Policy Authority 6/12/2007.
2.0	8-15-2007	Anderson	Section 2.8.5; Added language as to steps taken upon receipt of a subpoena requesting confidential information; Section 3.1.4; added language to clarify composition of DN; Section 4.6.7; Added procedures regarding CA archive information; Section 6.3.1; correct reference; Appendix 1: update revocation procedures to remove LDAP removal step;	Audit recommendation
2.0	8-28-2007	Anderson	Approved version	Approved via email vote 8/28/2007 by PA.
3.0	8/08/2008	Anderson	Convert CPS to new IETF RFC 3647 format	
3.0	10/24/2008	Anderson	Convert CPS to new IETF RFC	Further modifications to

			3647 format	language.
3.0	10/30/2008	Anderson, Christensen	Convert CPS to new IETF RFC 3647 format	Further modifications to language
3.1	3/16/2009	Policy Authority	Approve	CPS approved in RFC3647 format; version number modified to match CP version.

## Table of Contents

<b>1.</b>	<b>INTRODUCTION .....</b>	<b>15</b>
<b>1.1</b>	<b>OVERVIEW.....</b>	<b>16</b>
1.1.1	Certificate Policy (CP) .....	16
1.1.2	Relationship between the Illinois CP & the Illinois CPS .....	16
1.1.3	Relationship between the Illinois CP and Entity CP .....	16
1.1.4	Scope.....	17
1.1.5	Interaction with PKIs External to the State of Illinois .....	17
<b>1.2</b>	<b>DOCUMENT NAME &amp; IDENTIFICATION.....</b>	<b>17</b>
<b>1.3</b>	<b>PKI PARTICIPANTS.....</b>	<b>18</b>
1.3.1	Certification Authorities .....	19
1.3.2	Registration Authority (RA) .....	21
1.3.3	Subscribers .....	21
1.3.4	Relying Parties.....	21
1.3.5	Other Participants .....	22
<b>1.4</b>	<b>CERTIFICATE USAGE.....</b>	<b>22</b>
1.4.1	Appropriate Certificate Uses .....	22
1.4.2	Prohibited Certificate Uses.....	22
1.4.3	Appropriate Certificate Usage per Assurance Level .....	23
<b>1.5</b>	<b>POLICY ADMINISTRATION.....</b>	<b>23</b>
1.5.1	Organization administering the document.....	23
1.5.2	Contact Person .....	23
1.5.3	Person Determining Certification Practices Statement Suitability for the Policy .....	23
1.5.4	CPS Approval Procedures .....	23
<b>1.6</b>	<b>DEFINITIONS AND ACRONYMS.....</b>	<b>24</b>
<b>2.</b>	<b>PUBLICATION AND REPOSITORY RESPONSIBILITIES .....</b>	<b>25</b>
<b>2.1</b>	<b>REPOSITORIES.....</b>	<b>25</b>

2.1.1	Repository Obligations .....	25
<b>2.2</b>	<b>PUBLICATION OF CERTIFICATION INFORMATION.....</b>	<b>25</b>
2.2.1	Publication of Certificates and Certificate Status .....	25
2.2.2	Publication of CA Information.....	26
2.2.3	Interoperability .....	26
<b>2.3</b>	<b>FREQUENCY OF PUBLICATION .....</b>	<b>26</b>
<b>2.4</b>	<b>ACCESS CONTROLS ON REPOSITORIES.....</b>	<b>26</b>
<b>3.</b>	<b>IDENTIFICATION AND AUTHENTICATION .....</b>	<b>27</b>
<b>3.1</b>	<b>NAMING .....</b>	<b>27</b>
3.1.1	Types of Names .....	27
3.1.2	Need for Names to Be Meaningful .....	28
3.1.3	Anonymity or Pseudonymity of Subscribers.....	28
3.1.4	Rules for Interpreting Various Name Forms.....	28
3.1.5	Uniqueness of Names.....	28
3.1.6	Recognition, Authentication, & Role of Trademarks.....	28
<b>3.2</b>	<b>INITIAL IDENTITY VALIDATION .....</b>	<b>28</b>
3.2.1	Method to Prove Possession of Private Key .....	29
3.2.2	Authentication of Organization Identity.....	29
3.2.3	Authentication of Individual Identity.....	30
3.2.4	Non-verified Subscriber Information.....	32
3.2.5	Validation of Authority .....	32
3.2.6	Criteria for Interoperation .....	32
<b>3.3</b>	<b>IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS .....</b>	<b>32</b>
3.3.1	Identification and Authentication for Routine Re-key .....	32
3.3.2	Identification and Authentication for Re-key after Revocation.....	33
<b>3.4</b>	<b>IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST .....</b>	<b>33</b>
<b>4.</b>	<b>CERTIFICATE LIFE-CYCLE.....</b>	<b>35</b>
<b>4.1</b>	<b>APPLICATION.....</b>	<b>35</b>
4.1.1	Application of Behalf of a Device, Software Application, or process .....	36

4.1.2	Application for a Cross Certificate .....	36
<b>4.2</b>	<b>CERTIFICATE APPLICATION PROCESSING .....</b>	<b>37</b>
4.2.1	Performing Identification and Authentication Functions .....	37
4.2.2	Approval or Rejection of Certificate Applications .....	37
4.2.3	Time to Process Certificate Applications.....	37
<b>4.3</b>	<b>ISSUANCE .....</b>	<b>38</b>
4.3.1	CA Actions during Certificate Issuance .....	38
4.3.2	Notification to Subscriber of Certificate Issuance.....	38
<b>4.4</b>	<b>CERTIFICATE ACCEPTANCE .....</b>	<b>38</b>
4.4.1	Conduct constituting certificate acceptance .....	39
4.4.2	Publication of the Certificate by the CA.....	39
4.4.3	Notification of Certificate Issuance by the CA to other entities.....	39
<b>4.5</b>	<b>KEY PAIR AND CERTIFICATE USAGE.....</b>	<b>39</b>
4.5.1	Subscriber Private Key and Certificate Usage .....	39
4.5.2	Relying Party Public key and Certificate Usage [Old §2.1.4].....	39
<b>4.6</b>	<b>CERTIFICATE RENEWAL .....</b>	<b>40</b>
4.6.1	Circumstance for Certificate Renewal .....	40
4.6.2	Who may request Renewal .....	40
4.6.3	Processing Certificate Renewal Requests .....	41
4.6.4	Notification of new certificate issuance to Subscriber .....	41
4.6.5	Conduct constituting acceptance of a Renewal certificate .....	41
4.6.6	Publication of the Renewal certificate by the CA.....	41
4.6.7	Notification of Certificate Issuance by the CA to other entities.....	41
<b>4.7</b>	<b>CERTIFICATE RE-KEY.....</b>	<b>41</b>
4.7.1	Circumstance for Certificate Re-key .....	41
4.7.2	Who may request certification of a new public key .....	42
4.7.3	Processing certificate Re-keying requests .....	42
4.7.4	Notification of new certificate issuance to Subscriber .....	42
4.7.5	Conduct constituting acceptance of a Re-keyed certificate.....	42
4.7.6	Publication of the Re-keyed certificate by the CA .....	42
4.7.7	Notification of certificate issuance by the CA to other Entities .....	42

<b>4.8 MODIFICATION.....</b>	<b>42</b>
4.8.1 Circumstance for Certificate Modification.....	42
4.8.2 Who may request Certificate Modification.....	43
4.8.3 Processing Certificate Modification Requests .....	43
4.8.4 Notification of new certificate issuance to Subscriber .....	43
4.8.5 Conduct constituting acceptance of modified certificate .....	43
4.8.6 Publication of the modified certificate by the CA .....	43
4.8.7 Notification of certificate issuance by the CA to other Entities .....	43
<b>4.9 CERTIFICATE REVOCATION &amp; SUSPENSION .....</b>	<b>43</b>
4.9.1 Circumstance for Revocation .....	43
4.9.2 Who can request Revocation .....	44
4.9.3 Procedure for Revocation Request .....	44
4.9.4 Revocation Request Grace Period.....	45
4.9.5 Time within which CA must Process the Revocation Request .....	45
4.9.6 Revocation Checking Requirements for Relying Parties.....	45
4.9.7 CRL Issuance Frequency.....	45
4.9.8 Maximum Latency of CRLs .....	46
4.9.9 On-line Revocation/Status Checking Availability.....	46
4.9.10 On-line Revocation Checking Requirements .....	46
4.9.11 Other Forms of Revocation Advertisements Available .....	46
4.9.11.1 Checking requirements for other forms of revocation advertisements .....	46
4.9.12 Special Requirements Related To Key Compromise .....	46
4.9.13 Circumstances for Suspension .....	46
4.9.14 Who can Request Suspension.....	46
4.9.15 Procedure for Suspension Request .....	46
4.9.16 Limits on Suspension Period.....	47
<b>4.10 CERTIFICATE STATUS SERVICES.....</b>	<b>47</b>
4.10.1 Operational Characteristics.....	47
4.10.2 Service Availability .....	47
4.10.3 Optional Features .....	47
<b>4.11 END OF SUBSCRIPTION .....</b>	<b>47</b>

<b>4.12 KEY ESCROW &amp; RECOVERY.....</b>	<b>47</b>
4.12.1 Key Escrow and Recovery Policy and Practices .....	47
4.12.2 Session Key Encapsulation and Recovery Policy and Practices .....	47
<b>5. FACILITY MANAGEMENT &amp; OPERATIONS CONTROLS.....</b>	<b>48</b>
<b>5.1 PHYSICAL CONTROLS.....</b>	<b>48</b>
5.1.1 Site Location & Construction.....	48
5.1.2 Physical Access .....	48
5.1.3 Power and Air Conditioning.....	49
5.1.4 Water Exposures .....	49
5.1.5 Fire Prevention & Protection .....	49
5.1.6 Media Storage.....	50
5.1.7 Waste Disposal .....	50
5.1.8 Off-Site backup .....	50
<b>5.2 PROCEDURAL CONTROLS.....</b>	<b>50</b>
5.2.1 Trusted Roles.....	50
5.2.2 Number of Persons Required per Task.....	53
5.2.3 Identification and Authentication for Each Role.....	53
5.2.4 Separation of Roles.....	53
<b>5.3 PERSONNEL CONTROLS.....</b>	<b>54</b>
5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements .....	54
5.3.2 Background Check Procedures .....	55
5.3.3 Training Requirements.....	55
5.3.4 Retraining Frequency & Requirements .....	56
5.3.5 Job Rotation Frequency & Sequence .....	56
5.3.6 Sanctions for Unauthorized Actions .....	56
5.3.7 Independent Contractor Requirements .....	56
5.3.8 Documentation Supplied To Personnel.....	56
<b>5.4 AUDIT LOGGING PROCEDURES.....</b>	<b>56</b>
5.4.1 Types of Events Recorded.....	56
5.4.2 Frequency of Processing Log .....	57



5.4.3	Retention Period for Audit Logs .....	57
5.4.4	Protection of Audit Logs .....	57
5.4.5	Audit Log Backup Procedures.....	58
5.4.6	Audit Collection System (internal vs. external) .....	58
5.4.7	Notification to Event-Causing Subject .....	58
5.4.8	Vulnerability Assessments .....	58
<b>5.5</b>	<b>RECORDS ARCHIVE.....</b>	<b>58</b>
5.5.1	Types of Events Archived .....	58
5.5.2	Retention Period for Archive .....	59
5.5.3	Protection of Archive .....	59
5.5.4	Archive Backup Procedures.....	59
5.5.5	Requirements for Time-Stamping of Records .....	59
5.5.6	Archive Collection System (internal or external) .....	59
5.5.7	Procedures to Obtain & Verify Archive Information .....	60
<b>5.6</b>	<b>KEY CHANGEOVER.....</b>	<b>60</b>
5.6.1	Recovery at Subscriber Request .....	60
5.6.2	Involuntary Recovery at State Agency Request.....	60
5.6.3	Involuntary Recovery by Court Order.....	61
<b>5.7</b>	<b>COMPROMISE &amp; DISASTER RECOVERY .....</b>	<b>61</b>
5.7.1	Incident and Compromise Handling Procedures .....	62
5.7.2	Computing Resources, Software, and/Or Data Are Corrupted.....	62
5.7.3	Entity (CA) Private Key Compromise Procedures .....	62
5.7.4	Business Continuity Capabilities after a Disaster .....	62
5.7.5	System backup procedures.....	62
<b>5.8</b>	<b>CA &amp; RA TERMINATION .....</b>	<b>63</b>
<b>6.</b>	<b>TECHNICAL SECURITY CONTROLS .....</b>	<b>64</b>
<b>6.1</b>	<b>KEY PAIR GENERATION &amp; INSTALLATION .....</b>	<b>64</b>
6.1.1	Key Pair Generation.....	64
6.1.2	Private Key Delivery to Subscriber .....	65
6.1.3	Public Key Delivery to Certificate Issuer .....	65
6.1.4	CA Public Key Delivery to Relying Parties .....	66

6.1.5	Key Sizes .....	66
6.1.6	Public Key Parameters Generation and Quality Checking .....	66
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field) .....	66
<b>6.2</b>	<b>PRIVATE KEY PROTECTION &amp; CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS.....</b>	<b>66</b>
6.2.1	Cryptographic Module Standards & Controls .....	66
6.2.2	Private Key Multi-Person Control .....	67
6.2.3	Private Key Escrow .....	67
6.2.4	Private Key Backup [Old §6.2.4] .....	67
6.2.5	Private Key Archival .....	68
6.2.6	Private Key Transfer into or from a Cryptographic Module [Old §6.2.6] .....	68
6.2.7	Private Key Storage on Cryptographic Module .....	69
6.2.8	Method of Activating Private Keys .....	69
6.2.9	Methods of Deactivating Private Keys.....	69
6.2.10	Method of Destroying Private Keys.....	69
6.2.11	Cryptographic Module Rating.....	69
<b>6.3</b>	<b>OTHER ASPECTS OF KEY MANAGEMENT .....</b>	<b>69</b>
6.3.1	Public Key Archival .....	69
6.3.2	Certificate Operational Periods/Key Usage Periods.....	70
<b>6.4</b>	<b>ACTIVATION DATA .....</b>	<b>70</b>
6.4.1	Activation Data Generation & Installation.....	70
6.4.2	Activation Data Protection.....	70
6.4.3	Other Aspects of Activation Data .....	71
<b>6.5</b>	<b>COMPUTER SECURITY CONTROLS .....</b>	<b>71</b>
6.5.1	Specific Computer Security Technical Requirements .....	71
6.5.2	Computer Security Rating .....	72
<b>6.6</b>	<b>LIFE-CYCLE SECURITY CONTROLS.....</b>	<b>72</b>
6.6.1	System Development Controls.....	72
6.6.2	Security Management Controls.....	72
6.6.3	Life Cycle Security Ratings .....	72
<b>6.7</b>	<b>NETWORK SECURITY CONTROLS .....</b>	<b>72</b>

6.7.1	Cryptographic module protection .....	73
6.7.2	Cryptographic Module Engineering Controls.....	73
<b>6.8</b>	<b><i>TIME STAMPING</i> .....</b>	<b>73</b>
<b>7.</b>	<b>CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT .....</b>	<b>74</b>
<b>7.1</b>	<b><i>CERTIFICATE PROFILE</i>.....</b>	<b>74</b>
7.1.1	Version Numbers .....	74
7.1.2	Certificate Extensions .....	74
7.1.3	Algorithm Object Identifiers .....	88
7.1.4	Name Forms .....	89
7.1.5	Name Constraints .....	89
7.1.6	Certificate Policy Object Identifier .....	89
7.1.7	Usage of Policy Constraints Extension .....	89
7.1.8	Policy Qualifiers Syntax & Semantics .....	89
7.1.9	Processing Semantics for the Critical Certificate Policy Extension .....	89
<b>7.2</b>	<b><i>CRL PROFILE</i> .....</b>	<b>89</b>
7.2.1	Version Numbers .....	90
7.2.2	CRL Entry Extensions .....	90
<b>7.3</b>	<b><i>OCSP PROFILE</i> .....</b>	<b>91</b>
<b>8.</b>	<b>COMPLIANCE AUDIT AND OTHER ASSESSMENTS .....</b>	<b>92</b>
<b>8.1</b>	<b><i>FREQUENCY OF AUDIT OR ASSESSMENTS</i> .....</b>	<b>92</b>
<b>8.2</b>	<b><i>IDENTITY &amp; QUALIFICATIONS OF ASSESSOR</i>.....</b>	<b>92</b>
<b>8.3</b>	<b><i>ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY</i>.....</b>	<b>92</b>
<b>8.4</b>	<b><i>TOPICS COVERED BY ASSESSMENT</i> .....</b>	<b>92</b>
<b>8.5</b>	<b><i>ACTIONS TAKEN AS A RESULT OF DEFICIENCY</i> .....</b>	<b>94</b>
<b>8.6</b>	<b><i>COMMUNICATION OF RESULTS</i> .....</b>	<b>95</b>
<b>9.</b>	<b>OTHER BUSINESS AND LEGAL MATTERS .....</b>	<b>96</b>
<b>9.1</b>	<b><i>FEES</i>.....</b>	<b>96</b>
9.1.1	Certificate Issuance/Renewal Fees.....	96

9.1.2	Certificate Access Fees .....	96
9.1.3	Revocation or Status Information Access Fee .....	96
9.1.4	Fees for other Services .....	96
9.1.5	Refund Policy .....	96
<b>9.2</b>	<b>FINANCIAL RESPONSIBILITY.....</b>	<b>96</b>
9.2.1	Insurance Coverage.....	96
9.2.2	Other Assets .....	97
9.2.3	Insurance/warranty Coverage for End-Entities.....	97
<b>9.3</b>	<b>CONFIDENTIALITY OF BUSINESS INFORMATION .....</b>	<b>97</b>
9.3.1	Scope of Confidential Information .....	97
9.3.2	Information not within the scope of Confidential Information.....	98
9.3.3	Responsibility to Protect Confidential Information .....	98
<b>9.4</b>	<b>PRIVACY OF PERSONAL INFORMATION .....</b>	<b>98</b>
9.4.1	Privacy Plan .....	98
9.4.2	Information treated as Private .....	98
9.4.3	Information not deemed Private .....	98
9.4.4	Responsibility to Protect Private Information.....	98
9.4.5	Notice and Consent to use Private Information.....	98
9.4.6	Disclosure Pursuant to Judicial/Administrative Process.....	98
9.4.7	Other Information Disclosure Circumstances.....	99
<b>9.5</b>	<b>INTELLECTUAL PROPERTY RIGHTS.....</b>	<b>99</b>
<b>9.6</b>	<b>REPRESENTATIONS &amp; WARRANTIES.....</b>	<b>99</b>
9.6.1	CA Representations and Warranties.....	99
9.6.2	RA Representations and Warranties.....	100
9.6.3	Subscriber Representations and Warranties.....	100
9.6.4	Relying Parties Representations and Warranties.....	101
9.6.5	Representations and Warranties of other Participants .....	101
<b>9.7</b>	<b>DISCLAIMERS OF WARRANTIES .....</b>	<b>101</b>
<b>9.8</b>	<b>LIMITATIONS OF LIABILITY .....</b>	<b>101</b>
9.8.1	CA liability .....	101

9.8.2	RA liability .....	101
<b>9.9</b>	<b>INDEMNITIES.....</b>	<b>101</b>
9.9.1	Hold Harmless: Relying Parties .....	102
9.9.2	Hold Harmless: Subscribers.....	102
<b>9.10</b>	<b>TERM &amp; TERMINATION .....</b>	<b>103</b>
9.10.1	Term.....	103
9.10.2	Termination .....	103
9.10.3	Effect of Termination and Survival .....	103
<b>9.11</b>	<b>INDIVIDUAL NOTICES &amp; COMMUNICATIONS WITH PARTICIPANTS.....</b>	<b>103</b>
<b>9.12</b>	<b>AMENDMENTS .....</b>	<b>104</b>
9.12.1	Procedure for Amendment.....	104
9.12.2	Notification Mechanism and Period.....	104
9.12.3	Circumstances under which OID must be changed .....	104
<b>9.13</b>	<b>DISPUTE RESOLUTION PROVISIONS.....</b>	<b>104</b>
<b>9.14</b>	<b>GOVERNING LAW.....</b>	<b>105</b>
<b>9.15</b>	<b>COMPLIANCE WITH APPLICABLE LAW.....</b>	<b>105</b>
<b>9.16</b>	<b>MISCELLANEOUS PROVISIONS.....</b>	<b>105</b>
9.16.1	Entire agreement .....	105
9.16.2	Assignment .....	105
9.16.3	Severability .....	105
9.16.4	Enforcement (Attorney Fees/Waiver of Rights).....	105
9.16.5	Force Majeure.....	106
<b>9.17</b>	<b>OTHER PROVISIONS.....</b>	<b>106</b>
<b>10.</b>	<b>BIBLIOGRAPHY .....</b>	<b>107</b>
<b>11.</b>	<b>ACRONYMS AND ABBREVIATIONS .....</b>	<b>109</b>
<b>12.</b>	<b>GLOSSARY.....</b>	<b>112</b>
<b>13.</b>	<b>APPENDIX 1 – CERTIFICATE REVOCATION PROCEDURES .....</b>	<b>125</b>
<b>14.</b>	<b>APPENDIX 2 – FIPS 140-1 Validation Certificate .....</b>	<b>142</b>



# 1. INTRODUCTION

This introduction is intended to be a layman's description of the State of Illinois Public Key Infrastructure (PKI). This section is not intended to describe the policies and procedures that govern PKI. Policies and procedures are described in Sections 2 through 8 of this document and those sections govern all PKI operations.

The State of Illinois has created a Public Key Infrastructure to facilitate development of electronic applications that could replace many of the paper processes currently employed by the State's agencies. This document and the associated Certification Practice Statement describe the policies and procedures that govern operation of the State of Illinois PKI. PKI provides tools that can identify users to an electronic application, that can help enforce or apply confidentiality and privacy requirements, and that provides electronic signatures that comply with the Federal E-Sign Act and the State of Illinois' Electronic Commerce Security Act (5 ILCS 175).

A Public Key Infrastructure includes many participating entities. The Certification Authority (CA) for the State of Illinois PKI is operated by the Department of Central Management Services. Policies and procedures for PKI are developed and approved by the Policy Authority (PA), which includes representatives from several State agencies. Subscribers are individuals who register and are issued digital certificates. A Relying Party is an entity that uses the digital certificates as part of an electronic process.

Public Key Infrastructure uses the technology of public key encryption to provide functionality to users and applications. Users (whether individuals, electronic applications, or devices) are registered and two encryption keys are created – one held privately by the user and one made publicly available. The keys are mathematically related in that each operates as the inverse of the other, however the value of one key cannot be determined by analyzing the other. The public key is also contained in the digital certificate, which is issued to the user by CA. This digital certificate contains information which identifies the user to the Certificate Authority (CA) and links the user's keys to that identity. The State of Illinois PKI operates using a model commonly referred to as a "dual key pair" in which registered users are issued one digital certificate consisting of a corresponding public/private key pair for encryption and a second corresponding public/private key pair for signature purposes. Data that is encrypted using a given public key can only be decrypted using the corresponding private key. Likewise, a digital signature created using a given private key can only be verified by using the corresponding public key.

Digital certificates that are issued by Certificate Authorities (CA's) are identified according to how rigorously the user is authenticated during the registration process. This identification is called the assurance level and can be used to

determine whether a certificate can be relied on as part of a given process. High risk or highly sensitive transactions typically require a higher assurance level while a lower level of assurance may suffice for more mundane processes.

Subsequent sections of this document describe requirements, obligations, and procedures for each participant in PKI. More detailed and specific descriptions of the procedures are included in the associated Certification Practice Statement.

## **1.1 OVERVIEW**

This Certification Practice Statement (CPS) describes the practices of the Certificate Authority (CA) operated by the State of Illinois Central Management Services (“State”). This CPS is applicable to all entities with relationships with the State CA, including end users, Registration Authorities (RAs) and Local Registration Authorities (LRAs). This CPS provides those entities with a clear statement of the practices and responsibilities of the State CA, as well as the responsibilities of each entity in dealing with the State CA.

Section 25-105 of the Illinois Electronic Commerce Security Act (5 ILCS 175/25-105) provides that the Illinois Department of Central Management Services (CMS) will have the exclusive authority to specify the policies and procedures for the issuance and use of digital signatures by State Agencies. The Certificate Policy (CP) and the Certification Practices Statement (CPS) are CMS’s written description of the policies and procedures for the issuance and use of digital signatures. The Director of CMS has delegated responsibility for implementation and maintenance of the CP and the CPS to the State of Illinois Certificate Policy Authority (PA).

### **1.1.1 Certificate Policy (CP)**

Each of the Certificate Policies supported by the State CA, and covered by this CPS, identifies the suitable applications for that Certificate Policy.

### **1.1.2 Relationship between the Illinois CP & the Illinois CPS**

This CPS is called the State of Illinois Certificate Authority Certification Practices Statement for Digital Signatures and Encryption Applications. It is the supporting ‘how to’ document to the governing Illinois PKI certificate policy. This CPS is administered by the State PKI Operational Authority (OA) and is based on the policies agreed to by the State PKI Policy Authority (PA).

### **1.1.3 Relationship between the Illinois CP and Entity CP**

The Illinois Policy Authority maps Entity CP(s) to one or more of the levels of assurance in the Illinois CP. The relationship between those CPs and the Illinois Root CA shall be asserted in CA certificates in the *policyMappings* extension.



#### **1.1.4 Scope**

This CPS is managed by the State of Illinois Operational Authority (OA) and adheres to the policies established by the State of Illinois Policy Authority (PA). Contact information for these authorities is provided in section 1.5.2 below.

This CPS is applicable to all Certificates issued by the State CA, including those issued under the 'Certificate Policy for Digital Signature and Encryption Applications' policy.

The practices described in the CPS apply to the issuance and use of Certificates and Certificate Revocation Lists (CRLs) for users within the State CA domain.

#### **1.1.5 Interaction with PKIs External to the State of Illinois**

No Stipulation.

### **1.2 DOCUMENT NAME & IDENTIFICATION**

This CPS is called the State of Illinois Certificate Authority Certification Practice Statement for Digital Signature and Encryption Applications.

This CPS is managed by the State of Illinois Operational Authority (OA) and adheres to the policies established by the State of Illinois Policy Authority (PA). Contact information for these authorities is provided in section 1.4 below.

The State CA issues Certificates for use in verification of digital signatures and Certificates for use in encryption. The State CA supports several Certificate Policies that cover both of these applications. Practices that differ from this policy are clearly indicated in this CPS. The Certificate Policies supported by the State CA and for which its practices are described in this CPS is identified below:

Certificate Policies for Digital Signature and Encryption Applications

Level 1 (software)	2.16.840.114273.1.1.1.1
Level 1 (hardware)	2.16.840.114273.1.1.1.2
Level 2 (software)	2.16.840.114273.1.1.1.3
Level 2 (hardware)	2.16.840.114273.1.1.1.4
Level 3 (software)	2.16.840.114273.1.1.1.5
Level 3 (hardware)	2.16.840.114273.1.1.1.6
Level 4 (hardware only)	2.16.840.114273.1.1.1.7
MEDI Single-Use Certificate	2.16.840.114273.1.1.2.1

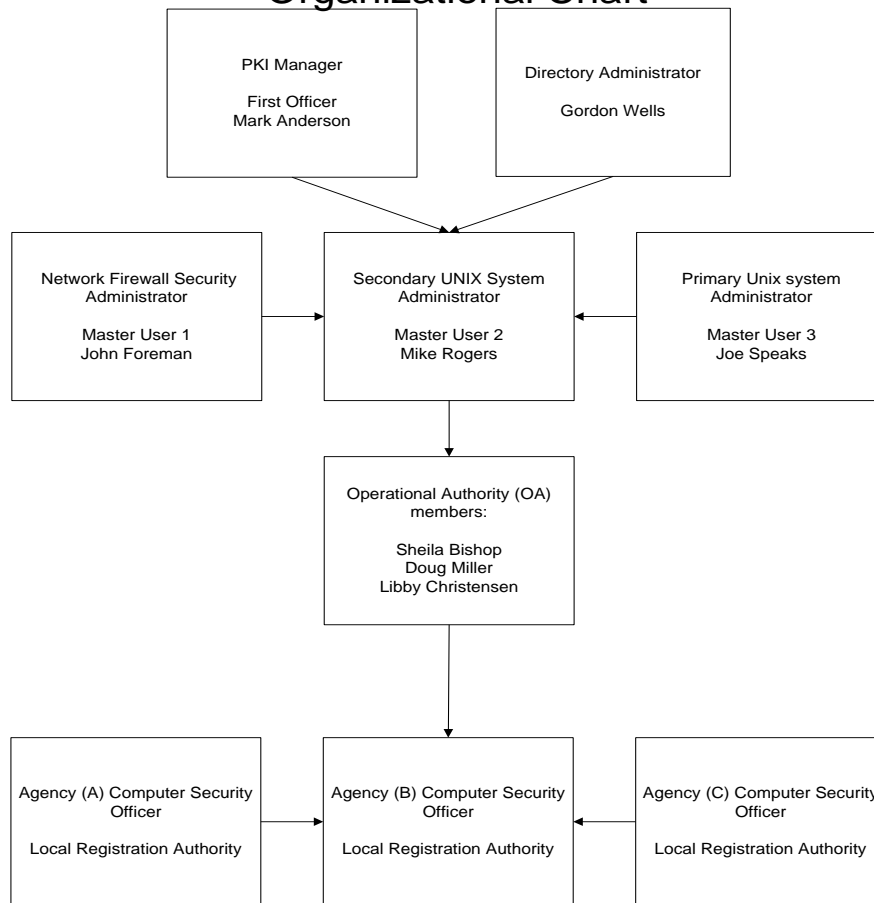
### **1.3 PKI PARTICIPANTS**

The sub-sections that follow describe in general terms, the functions of the major components of the PKI.

There is created by the CP and this CPS a State of Illinois Operational Authority (OA.) The Director of CMS will have supervisory responsibility for the OA. The OA will be responsible for interpretation of the certificate policies as stated by the PA, the creation and management of the CPS, and the correct operation of the State PKI, in accordance with the provisions of the CP and the CPS. The CMS Security Administrator will oversee the operations of the State PKI. The CMS PKI registration authority (RA) will manage the operations of the State PKI. CA functions described in the CP and the CPS will be performed by PKI Administrators. Registration Authority functions described in the CP and CPS may be delegated to Local Registration Authorities (LRAs.) Figure 1 illustrates the CMS organizational structure relating to the operation and management of the State CA.

In the State PKI, there are three Master Users who also serve as System Administrators. The OA manager will have Security Officer privileges. The PKI Operational Authority staff has Administrator privileges. The Agency/entity Local Registration Authorities are limited to performing Registration Authority functions while the CMS Internal Auditors and External Auditors would be granted read-only access.

# State Of Illinois PKI Organizational Chart



## 1.3.1 Certification Authorities

The State operates a single CA, which issues user Certificates to State Employees and other entities which conduct business with the State.

The State CA is operated using Entrust release 7.0 software and the CA is represented in the architecture by Entrust/Security Manager™. The authorized State personnel access Entrust/Security Manager™ via the Entrust/SMA interface to initiate and perform CA functions.

### 1.3.1.1 Policy Authority (“PA”)

The State of Illinois Policy Authority is responsible for the certificate policy that governs this CPS. This CPS is updated by the OA to align practices with new or revised policy requirements released by the PA. The OA will continue to operate from the latest approved CPS until the PA has approved and issued the updated CPS to the OA.

The PA will be comprised of representatives of participating units of Illinois State government. The Director of CMS will have the exclusive authority to appoint

and remove members of the PA. Members of the PA (or their designees) will have the authority to implement, maintain, and modify the CP and the CPS, and will perform all other duties required of them by the terms of the CP and the CPS.

#### **1.3.1.2 Operational Authority (“OA”)**

The following chart illustrates the relationships of CMS individuals to PKI roles.

<b>State Individual</b>	<b>Entrust Role</b>
PKI Manager/Certificate Authority Administrator/Program Manager, Central Management Services	Security Officer
Directory Administrator, Central Management Services	CMS Administrator
Firewall Administrator	Master User 1
SUN System Administrator	Master User 2
Primary UNIX System Administrator	Master User 3
PKI System Administrator Registration Authority	CMS Administrator
Agency Assigned Individual	LRA
State Employees and Business Partner Users	End user

Where necessary, this CPS distinguishes the different users and roles accessing Entrust/Security Manager™ for CA functions. Where this distinction is not required, the term CA is used to refer to the total CA entity, including the software and its operations.

#### **1.3.1.3 Illinois Operational Authority Program Manager**

The Program Manager is the individual within the Illinois PKI Operational Authority who has principal responsibility for overseeing the proper daily operation of the Illinois PKI in accordance with this CPS.

#### **1.3.1.4 Entity Principal Certification Authority (CA)**

This entity is responsible for the day to day operation of the Illinois PKI, and for ensuring its availability to its subscribers, customers, and relying parties. As such, this entity has high privileges that allow them to perform these functions.

#### **1.3.1.5 Certificate Status Servers**

No Stipulation.

### **1.3.2 Registration Authority (RA)**

The Registration Authority has privileges that are a proper subset of the Security Officer privileges as outlined in section 5.2.1 of this CPS. The State RA makes use of authorized individuals to function as Local Registration Authorities to verify the identity and roles of End Entities throughout the various State agencies and business partners, in accordance with the State of Illinois Certificate Policy.

#### **1.3.2.1 Local Registration Authority**

Each Agency will designate one or more individuals to perform the role of the Local Registration Authority within that agency, and has privileges that are a proper subset of Security Officer privileges as outlined in section 5.2.1 of this CPS. In this CPS, the term Local Registration Authority (LRA) is used to refer to an individual performing RA functions, while RA is used to refer to the total RA entity, including the software and its operations.

### **1.3.3 Subscribers**

This CPS will be binding on each Subscriber that applies for and/or obtains Certificates, by virtue of the Subscriber Agreement, and governs each applicant's performance with respect to their application for, use of, and reliance on, Certificates issued by the CA. The Subscriber agreement may be viewed at [http://www.illinois.gov/pki/pki\\_subscriber.cfm](http://www.illinois.gov/pki/pki_subscriber.cfm).

#### **1.3.3.1 End Entities**

End-Entities in this PKI may include State employees, individuals conducting electronic business with the State, hardware devices and/or specific applications. At the discretion of the PA, any person entity, hardware device or specific application may be a Subscriber (relying party taken out) (collectively referred to as an "End Entity") in the State PKI. End-Entities may also use Certificates issued by the CA to encrypt information for, and verify the digital signatures of, other End-Entities within the State PKI.

### **1.3.4 Relying Parties**

An entity that needs to rely on a certificate issued by the State of Illinois PKI, but chooses not to use the Illinois recommended products for certificate verification and validation, is defined by the State of Illinois as a relying party. These entities

are in a position to rely on the certificates presented to them, and have agreed to be bound by the terms of the CP. The term “Relying Parties” is also used for entities that wish to use State of Illinois certificates, but do not wish to use any of the software available from the State PKI. In these instances, the entity is responsible for all certificate verification, including certificate revocation list checking, certificate validation date checking and any checks necessary to validate the trustworthiness of the end user certificate. These entities must sign a Relying Party agreement as provided by the State PKI.

By accepting a certificate issued pursuant to the provisions of this CP, a relying party agrees to be bound by the provisions of the CP. The following factors, among others are significant in evaluating the reasonableness of a recipient’s reliance upon a certificate, and upon digital signatures verifiable with reference to the public key listed in the certificate:

- Facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference;
- The value or importance of the digitally signed message, if known;
- The course of dealing between the relying person and the subscriber, and the available indicia of reliability or unreliability apart from the digital signature;
- The usage of trade, particularly trade conducted by trustworthy systems or other computer based means.

### **1.3.5 Other Participants**

No stipulation.

## **1.4 CERTIFICATE USAGE**

### **1.4.1 Appropriate Certificate Uses**

This CPS is applicable to all Certificates issued by the State CA, including those issued under the ‘Certificate Policy for Digital Signature and Encryption Applications’ policy. The practices described in the CPS apply to the issuance and use of Certificates and Certificate Revocation Lists (CRLs) for users within the State CA domain.

### **1.4.2 Prohibited Certificate Uses**

Each of the Certificate Policies supported by the State CA, and covered by this CPS, identifies the suitable applications for that Certificate Policy. Any use of the State of Illinois certificate used in any illegal activities or illegal gains is prohibited and if detected the certificate shall be revoked according to the procedures set forth in this CPS. State of Illinois certificates are to be used only for use of and/or interaction with Illinois Governmental entities, and not for private use.

### **1.4.3 Appropriate Certificate Usage per Assurance Level**

The Illinois PKI allows the user entities to make the final determination as to the assurance level needed by their applications. Suggestions are provided in the CP in section 1.4.3.

## **1.5 POLICY ADMINISTRATION**

The State of Illinois Policy Authority is responsible for the certificate policy that governs this CPS. This CPS is updated by the OA to align practices with new or revised policy requirements released by the PA. The OA will continue to operate from the latest approved CPS until the PA has approved and issued the updated CPS to the OA.

### **1.5.1 Organization administering the document**

This CPS is administered by the State PKI Operational Authority (OA) and is based on the policies agreed to by the State PKI Policy Authority (PA).

### **1.5.2 Contact Person**

The contact details for this CPS and PKI are:

Val Falzone

State of Illinois PKI Policy Authority Chairperson

1021 North Grand Ave. East

Springfield, IL 62794

Val.Falzone@epa.state.il.us

Telephone: 217-785-1605

Fax:

### **1.5.3 Person Determining Certification Practices Statement Suitability for the Policy**

This Certification Practice Statement is administered by the PA. The Operational Authority is responsible for operating the components of the Illinois PKI in compliance of this CPS as defined by the requirements stated in the Certificate Policy (CP). This will be done via a vote and approval process on all proposed changes.

The PA is responsible for approving and authorizes any CPS before the OA is bound by its guidance.

### **1.5.4 CPS Approval Procedures**

In order to allow entities to modify their procedures as needed, all changes to this document will become effective 30 days after final publication on the State Repository (<http://www.illinois.gov/pki>). It will be the responsibility of each

Subscriber or Relying Party to periodically check this Repository for notices associated with this document and Illinois PKI activities. The use of or reliance upon a certificate after the 30-day comment period, regardless of when the certificate was issued, will be deemed acceptance of the modified terms and therefore binding arbitration has occurred by the parties.

The State PA approves this CPS. The State PA must approve any subsequent changes prior to promulgation or activities performed by the OA. The express waiver by the State or the Policy Authority of any provision, condition, or requirement of this CPS will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

## ***1.6 DEFINITIONS AND ACRONYMS***

See Sections 11 and 12.



## **2. PUBLICATION AND REPOSITORY RESPONSIBILITIES**

CMS will maintain a Certificate Repository containing information pertaining to State Certificates.

### **2.1 REPOSITORIES**

The repository for the Illinois Root CA is provided by an X.500 directory system. The protocol used to access the Directory is the Lightweight Directory Access Protocol (LDAP) version 2 or higher.

The syntax of an LDAP call from a web browser to the repository to retrieve information is as follows:

Ldap://server.cmc.state.il.us:389/full DN of object being retrieved.

The public LDAP repository will contain public keys and certificate revocation lists, as well as profiles (doubly encrypted) for roaming users.

A public website is also maintained which contains links, policies, etc vital to the PKI community. This website is located at [www.illinois.gov/pki](http://www.illinois.gov/pki).

#### **2.1.1 Repository Obligations**

The Entrust software contains an internal database that immediately publishes information to a public LDAP repository that supports the State PKI and maintains availability, reliability, and sufficient protections for its contents. The public LDAP repository will contain public keys and certificate revocation lists, as well as profiles (doubly encrypted) for roaming users.

A public website is also maintained which contains links, policies, etc vital to the PKI community. This website is located at [www.illinois.gov/pki](http://www.illinois.gov/pki).

### **2.2 PUBLICATION OF CERTIFICATION INFORMATION**

This detailed CPS is not published publicly.

- The following PKI information is published in the State Directory:
- all encryption public key Certificates issued by the State CA to PKI users;
- all revocations of PKI user public key Certificates performed by the State CA;
- all public verification keys;
- all revocations of cross-certification certificates issued by the CA.
- Roaming profiles

#### **2.2.1 Publication of Certificates and Certificate Status**

This CPS is re-issued and published as necessary. Certificates are published in the Directory as they are issued. CRLs are published in the Directory as they are issued. The frequency of CRL is discussed in Section 4.4.9 of this CPS

### **2.2.2 Publication of CA Information**

In order to allow entities to modify their procedures as needed, all changes to this document will become effective 30 days after final publication on the State Repository (<http://www.illinois.gov/pki> ). It will be the responsibility of each Subscriber or Relying Party to periodically check this Repository for notices associated with this document and Illinois PKI activities. The use of or reliance upon a certificate after the 30-day comment period, regardless of when the certificate was issued, will be deemed acceptance of the modified terms and therefore binding arbitration has occurred by the parties.

The State PA approves this CPS. The State PA must approve any subsequent changes prior to promulgation or activities performed by the OA. The express waiver by the State or the Policy Authority of any provision, condition, or requirement of this CPS will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

### **2.2.3 Interoperability**

Any certificates, CRLs, or other public information stored in the directory will be stored using standards based schemas for objects and attributes.

## **2.3 FREQUENCY OF PUBLICATION**

This CPS is re-issued and published as necessary. Certificates are published in the Directory as they are issued. CRLs are published in the Directory as they are issued. The frequency of CRL is discussed in Section 4.9.7 of this CPS.

## **2.4 ACCESS CONTROLS ON REPOSITORIES**

The State of Illinois Operational Authority will protect any information not intended for public dissemination or modification. Public keys and certificate status information in the State of Illinois repository will be publicly available through the Internet. The use of certificates to access information in Agency repositories will be determined by the Agency pursuant to its authorizing and controlling statutes.

The State of Illinois PKI utilizes shadow directories to make repository information available to subscribers, relying parties, and others who need access to public certificates or revocation lists. These shadow directories are read-only copies of the master repository, and are updated immediately as the master repository is updated.

### **3. IDENTIFICATION AND AUTHENTICATION**

Subject to the requirements noted below, applications for State Certificates may be communicated from the applicant to the State RA or a State LRA and authorizations to issue State Certificates may be communicated from an authorized State LRA to the State CA, (1) electronically, provided that all communication is secure, or (2) in person.

The State CA expects to process three types of registrations:

- Web registration (both in-state and out-of-state recipients).
- Face-to-face registration authorized by the State RA or a State LRA.
- Bulk registration. Using a secure means determined on a case by case basis, authorized LRAs will authorize the issuance of Certificates to large groups of Subscribers that they have registered and communicate these to the State RA.

#### **3.1 NAMING**

Subject to the requirements noted below, applications for State Certificates may be communicated from the applicant to the State RA or a State LRA and authorizations to issue State Certificates may be communicated from an authorized State LRA to the State CA, (1) electronically, provided that all communication is secure, or (2) in person.

The State CA expects to process three types of registrations:

- Web registration (both in-state and out-of-state recipients).
- Face-to-face registration authorized by the State RA or a State LRA.
- Bulk registration. Using a secure means determined on a case by case basis, authorized LRAs will authorize the issuance of Certificates to large groups of Subscribers that they have registered and communicate these to the State RA

##### **3.1.1 Types of Names**

Names for Certificate issuers and Certificate subjects are of the X.500 Distinguished Name (DN) form.

The format used by this Certificate Authority is as follows:

DN:serialNumber=99999999+cn=common  
name,ou=??,ou=People,ou=CMS,o=State of Illinois,c=US

Where: serialNumber=99999999 is an 8 digit number assigned by the OA to ensure uniqueness.

Cn=common name of the requestor

Ou=?? Is an organizational unit based on the first letter of the person's last name

All other attributes are constant. All attributes are as defined in ITU-T Recommendation X.521.

### **3.1.2 Need for Names to Be Meaningful**

The value of the commonName attribute used is the name by which the Certificate subject is commonly known within the client organization.

### **3.1.3 Anonymity or Pseudonymity of Subscribers**

The State of Illinois PKI does not allow Anonymity of subscribers. Certificate names of device certificates will be constructed so that the agency owning or responsible for the device is easily ascertained.

### **3.1.4 Rules for Interpreting Various Name Forms**

In a Certificate, the issuer DN and subject DN fields contain the full X.500 Distinguished Name of the Certificate issuer or Certificate subject. If the subjectAltName extension is present in a Certificate, it contains the Certificate subject's rfc822Name (email address).

### **3.1.5 Uniqueness of Names**

Names are unambiguously defined for each object in the naming hierarchy. The common name (cn) shall be a combination of first name(s) and surname. Middle initials and other identifiers may also be used. The serialNumber attribute within the DN is used to ensure that no two individuals are assigned the same DN, and therefore the same electronic identity {serialNumber must be a sequential counter number – 8 digits; devices may use MAC number from the network interface device}. This combination of serial number/MAC address plus the common name will guarantee uniqueness among the distinguished names.

### **3.1.6 Recognition, Authentication, & Role of Trademarks**

The Illinois PKI will not seek any evidence that a subject's name is a registered trademark.

## **3.2 INITIAL IDENTITY VALIDATION**

The RA and appropriate LRAs will accept certificate applications from state employees or individuals who need to conduct electronic business with the State of Illinois through three primary registration means: web, in-person and bulk applications.

Web registration is available for users of Agency-based web applications. The registration process is handled entirely through the internet, with the applicant providing necessary identification information on a web form. The RA validates the identity information provided by the applicant against one or more trusted data sources.

A web registration process is available for out-of-state residents who desire a State of Illinois digital certificate. This process instructs the recipient to download a form, take it to a notary public, present proper identification, and have the form notarized. This form is then mailed to the OA, where activation codes are created and distributed to the recipient in a secure manner. These codes are then entered into a secure web page to generate the certificate. All out-of-state certificates are created as a level 1 certificate as described in section 3.2.3.

In-person applications will be accepted by the RA or any authorized LRA. The applicant must submit a completed State of Illinois Digital Certificate Application in person at the time of application.

Bulk applications for state agency staff or other definable groups of individuals will be accepted by the RA from appropriate LRAs in accordance with procedures developed on a case by case basis. Certificates will be issued at the assurance level determined from evaluating the authentication provided by the bulk registration process using the authentication requirements described in Section 3.2.3.

For each Certificate application, prospective Subscribers will satisfy the following requirements:

- Provide proof of identity as required in Section 3.2.3
- Submit a completed State of Illinois Digital Certificate Application to the RA or appropriate LRA;
- Indicate agreement with the terms and conditions for use of the State's public key infrastructure as described in the Subscriber's Agreement;
- Initialize the client software on their workstation (if appropriate); and,
- Demonstrate to the RA that the private keys have been successfully installed.

### **3.2.1 Method to Prove Possession of Private Key**

Digital Certificates bind a public key to the identity of the individual to assure Relying Parties that encryption or signing performed by the private key was done by the individual whose public key appears on the Certificate. This requires that an individual safeguard their profile and Entrust password and that the CA require proof of possession of the private key before creating and signing a Certificate containing the associated public key. Proof of possession of private key is handled automatically by the operations of the PKIX.

For the signature private key, a PKIX operation initiated by the Subscriber is digitally signed using the signature private key itself.

For the decryption private key, this key is transferred to the Subscriber, together with the corresponding Certificate, in a PKIX operation, which is digitally signed by the State CA.

### **3.2.2 Authentication of Organization Identity**

The State of Illinois PKI does not issue certificate to organizations.

### **3.2.3 Authentication of Individual Identity**

The following sections detail the registration process to be used for issuance of State Certificates:

- **Face to Face Registration**  
The Subscriber will present themselves in person along with a valid form of photo identification (either a State of Illinois Driver's License or a Secretary of State Identification Card) and one other form of Id to either the RA or an LRA. The RA or LRA will validate the information and sign and date the form, which at a minimum will include:
  - Contains full name.
  - Driver's license number or Secretary of State Identification Number.

Shared secret information for key recovery. (Any shared secret information will be encrypted, hashed, stored securely, or otherwise physically protected.)

If an LRA conducts the registration, they will then securely forward the information on to the RA, who will then generate the certificates. If an LRA exists for the subscriber, the reference number and authorization code are encrypted, signed and emailed to the LRA. If no LRA exists, then one part of the necessary authorization credentials is emailed and another will be provided via some "out of band" method. The RA or LRA is responsible to provide the necessary credentials to subscribers who will be "desktop users". These two pieces of information are required for the Subscriber to authenticate and initialize themselves with the CA at their initial login.

If a subscriber is to be a "roaming user", then the digital certificate and the profile are both created under the user's control by the CA and the profile name and password are securely transmitted to the LRA or the subscriber as described above.

A face-to-face registration results in a level 2 authorization level unless a background check is also performed. In this case, a level 3 assurance level is assigned.

- If a biometric feature to protect the private keys is added to a level 3 assurance level, a level 4 assurance level is assigned.
- All registration forms will be securely retained indefinitely.
- All trusted roles must have at least a level 3 assurance level.

#### **Web registration**

Agencies can choose to include a link in their developed web applications which will route the subscriber to a State web page. This web page would allow the subscriber to fill out an on-line form and obtain a digital certificate. The subscriber will provide information, which the Agency's

application deems necessary as well as information found on the subscriber's drivers license and shared secret information. This driver's license information is then verified against the driver's license database housed at the Secretary of State. Currently, the information verified is the driver's license number and the weight as shown on the driver's license. If this information matches, then a digital certificate will be issued to the subscriber and they will be returned to the Agency's application that they started with. The shared secret information will be stored in a secure DB2 database housed at CMS for use in later key recovery operations.

- An out-of-state registration process has been added to the web registration model. Under this process, non-Illinois residents can request a State of Illinois digital certificate by going to the normal registration web site and choosing the "out-of-state" option. This option directs them to download and print an application form, and to take it to a notary public where their identification credentials are inspected. Once the form is notarized, it is mailed to the Operational Authority for processing. Once the activation codes are created by the Operational Authority, the activation codes are returned to the requestor via email and one "out-of-band" method. They are then directed to go to another web site and enter the activation codes, thus creating the certificate.
- The web registration model will only result in a level 1 assurance level.
- Other registration methods may be used that are consistent with the requirements of the CP and created with the approval of the Policy Authority.

A provision of cross-certification with the Federal Bridge requires subscribers to be re-authenticated after 9 years. Since the Illinois PKI is less than 9 years old, the procedures for accomplishing this will be determined in future discussions by the Policy Authority.

#### **3.2.3.1 Authentication of Human Subscribers**

Refer to section 3.2.3.

#### **3.2.3.2 Authentication of Human Subscribers For Group Certificates**

Illinois does not issue group certificates.

#### **3.2.3.3 Authentication of Devices**

Application for a device or an application to be an End-Entity must be made by an individual to whom the device or application's signature is attributable for the purposes of accountability and responsibility.

Identification and authentication of the applicant follows section 4.1.1 of the CP as if the organization or individual were applying for a Certificate on their own behalf. In addition, an LRA, the RA or PA must verify the authority of the

individual to receive Certificates for that device or application and authorize the issuance of the certificate. Identification and authentication procedures are dealt with in section 3.2.3 of this CPS.

Device certificates will be valid for 3 years. At this time, the viability of this certificate must be validated by the responsible LRA.

#### **3.2.4 Non-verified Subscriber Information**

Non-verifiable information will not be included in Illinois PKI certificates with the exception of the email address in subscriber certificates.

#### **3.2.5 Validation of Authority**

For cross-certification, the State of Illinois Policy Authority will validate the representative's authorization to act in the name of the organization. For device certificates, the Local Registration Authority will be validated before the certificate is issued by comparing the LRA signature to the list of valid LRA's maintained by the OA.

#### **3.2.6 Criteria for Interoperation**

No Stipulation.

### **3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS**

For cross-certification relationships, no automatic key update process is applied. If the State PA determines that a cross-certification agreement is to extend beyond the original period, a new cross-certificate is issued, prior to expiration of the current one. The same identification and authentication process used for initial cross-certification agreements applies to the issuance of new keys.

A provision of cross-certification with the Federal Bridge requires subscribers to be re-authenticated after 9 years. Since the Illinois PKI is less than 9 years old, the procedures for accomplishing this will be determined in future discussions by the Policy Authority.

#### **3.3.1 Identification and Authentication for Routine Re-key**

Once subscriber's keys enter the update or rekey transition period, the CA will automatically attempt to perform a key update the next time the subscriber uses their certification. This rekey process is a transparent operation to the subscriber and should cause no interruption of service or operational capabilities to the subscriber during the event. However, failure of the Subscriber to successfully remain connected to the CA to complete this key update process will result in their Certificate expiring. If that should occur, the Subscriber will have to repeat



the authentication processes defined in section 3.2.3 of this CPS or request a complete key recovery.

For all Certificate renewal requests, the Certificates are renewed using PKIX operations invoked by Entrust/Security Manager™. Authentication of the individual's identity as defined in section 3.2.3 of this CPS need not be repeated. However, re-authentication of an individual's identity will occur as described in section 3.3.1 of the CP.

#### **3.3.1.1 Routine Re-key – Device or Application**

Once the keys of a device or application enter the transition period, the CA will automatically attempt to perform a key update. This is a transparent operation that should cause no interruption of operation. Failure of the Subscriber to successfully connect to the CA to complete this key update during the transition period will result in their Certificate expiring and the Subscriber having to repeat the authentication process defined in section 3.2.3 of this CPS or have a key recovery operation performed by the OA.

For all Certificate renewal requests, the Certificates are renewed using PKIX operations invoked by Entrust/Security Manager™. Authentication of the individual's identity as defined in section 3.2.3 of this CPS need not be repeated. However, re-authentication of an individual's identity will occur as described in section 3.2.3 of the CP.

#### **3.3.2 Identification and Authentication for Re-key after Revocation**

For users whose Certificates have been revoked, recovery after revocation will generally not be permitted until the identification and authentication requirements for initial registration described in section 3.2.3 of this CPS are repeated. Local Registration Authorities may allow exceptions in the following situation:

- An certificate holder is temporarily unable to present themselves in person (e.g. on extended travel) and the revocation was not due to a key compromise.

### **3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST**

Requests by a Trusted Role to revoke a Certificate require Administrator privilege credentials to be supplied at login to Entrust/Authority™ before revocation requests can be serviced. Requests by the Subscriber to revoke their own Certificate require one of the following identification and authentication mechanisms prior to a Trusted Role initiating an online request:

- Subscriber presents themselves in person along with their photo id card;
- Email sent from the Subscriber to a Trusted Role.
- Email from an LRA or trusted role.

- Requests to revoke device and application certificates must be provided (via signed email or in person) by the LRA or Security Officer of the responsible agency.

A trustworthy, automated revocation process may replace or supplement the above-described manual process.

#### **3.4.1.1 *Involuntary recovery at governmental entity request***

- A Governmental entity may request involuntary recovery of a Subscriber's private encryption keys if that person is or has recently been employed by the entity, the entity has reason to believe that data necessary to agency operations has been encrypted using the Subscriber's keys, and the entity is unable to contact the Subscriber or the Subscriber is unable or unwilling to decrypt the data.
- The entity's request will be made in writing to the PA, describing why the Subscriber's private encryption key is necessary to entity operations and specifying what use will be made of the key. The request will be signed by the Director of the Agency. The Subscriber's keys will not be recovered until said request is reviewed by the PA or those designated by the PA to review such requests.
- Prior to recovering the Subscriber's profile, the CA will alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate will be recovered and the profile will be delivered to the entity LRA on physical media. The LRA will sign for receipt of the profile, will supervise all entity use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked.

No recovery will be performed until the request has been approved by the Policy Authority.

#### **3.4.1.2 *Involuntary recovery by court order***

- The PA and OA will comply with all official, authorized, and verified court orders to recover a Subscriber's keys.
- Prior to recovering the Subscriber's profile, the CA will alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate will be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA will sign for receipt of the profile, will supervise all Agency use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked.

## **4. CERTIFICATE LIFE-CYCLE**

### **4.1 APPLICATION**

Both the Reference Number and Authorization Code are required for the individual to initially login to the PKI system as a new user unless the user is created through the State of Illinois online registration system. A digital signature key pair is generated by the software on the client desktop and a Certificate request is sent to Entrust/Security Manager™ using the PKIX protocol.

The RA and appropriate LRAs can accept certificate applications from state employees or individuals who need to conduct electronic business with the State of Illinois through three primary registration means: web, in-person and bulk applications.

Web registration is available for users of Governmental-based web applications. The registration process is handled entirely through the internet, with the applicant providing necessary identification information on a web form. Information entered by the applicant (who must possess either a State of Illinois driver's license or identification card as issued by the Illinois Secretary of State) is validated in real time against the Secretary of State's driver's license database. All certificates are generated by the online process in real time as roaming certificates at a level 1 authentication level.

A partial web registration process is available for out-of-state residents who desire a State of Illinois digital certificate. This process instructs the recipient to download a form, take it to a notary public, present proper identification, and have the form notarized. This form is then mailed to the OA, where activation codes are created and distributed to the recipient in a secure manner. These codes are then entered into a secure web page to generate the certificate. All out-of-state certificates are created as a level 1 certificate as described in section 3.1.9.

In-person applications will be accepted by the RA or any authorized LRA. The applicant must submit a completed State of Illinois Digital Certificate Application in person at the time of application. Two valid forms of identification must be provided at the time of registration. In-person applications result in a level 2 certificate being issued.

Bulk applications for state agency staff or other definable groups of individuals will be accepted by the RA from appropriate LRAs in accordance with procedures developed on a case by case basis. Certificates will be issued at the assurance level determined from evaluating the authentication provided by the bulk registration process using the authentication requirements described in Section 3.2.3.

For each Certificate application, prospective Subscribers will satisfy the following requirements:

- Provide proof of identity as required in Section 3.2.3
- Submit a completed State of Illinois Digital Certificate Application to the RA or appropriate LRA;
- Indicate agreement with the terms and conditions for use of the State's public key infrastructure as described in the Subscriber's Agreement;
- Initialize the client software on their workstation (if appropriate); and,
- Demonstrate to the RA that the private keys have been successfully installed

#### **4.1.1 Application of Behalf of a Device, Software Application, or process**

The RA will accept certificate applications submitted on behalf of hardware devices and software applications or processes that are owned by the State of Illinois or operated by an external entity for the purpose of inter-operating with or operating on behalf of the State. Applications will be accepted from State employees or LRAs holding currently valid Certificates issued by this CA and will be signed by the appropriate LRA or the agency Director, if no agency LRA is available. The application must include appropriate identification information for the device, a description of the device, the name of the person responsible for maintaining the device, and the purpose that the certificate will serve if issued. For certificates issued to external entities, the application must also include the name of the State agency employee who is responsible for the ongoing relationship with the external entity, which requires the certificate.

#### **4.1.2 Application for a Cross Certificate**

Once the conditions of CP section 4.1.2 have been satisfied, the Operational Authority (OA) will perform the following actions for cross-certification:

- Obtain permission from the Policy Authority to proceed with cross-certification exercises
- Examine audit letter/report for possible compliance problems
- Perform policy mapping exercise based upon the application received, using the Illinois CP and the applicant's CP
- Report mapping inconsistencies to the Policy Authority for review and/or remediation with applicant
- Once policy mapping has been completed to the satisfaction of the Policy Authority, perform Directory interoperability testing
- Report results of Directory testing to the Policy Authority for recommendation/decision
- Policy Authority and applicant develop mutually agreeable Memorandum of Agreement (MOA)

- If directed by the Policy Authority, modify the master.certspec file for the new cross-certificate level of assurance (mapping Illinois certificate type to applicant's certificate type), and
- Jointly issue off-line cross-certificates with applicant.

## **4.2 CERTIFICATE APPLICATION PROCESSING**

Refer to section 3.2.3.

### **4.2.1 Performing Identification and Authentication Functions**

Digital certificates obtained through the State Internet registration process generate a (level 1) assurance level credential. If it becomes necessary to upgrade that certificate to a level 2 assurance level requires face-to-face verification, and the following steps will be followed:

Have the user/client fill out the following fields on the PKI Certificate Application form:

- Last Name
- First Name
- Middle Name
- Date of Birth
- Social Security Number
- Illinois Driver's license/State Identification card
- email address
- Requestor's signature
  - a. Perform the face-to-face verification as normal. Sign the form under "Local Registration Authority Signature".
  - b. Write "certificate upgrade" on the form in the bottom right corner.
  - c. Send the form to CMS as is currently done.

### **4.2.2 Approval or Rejection of Certificate Applications**

The Illinois OA may approve or reject certificate applications. Applications may be rejected if they are incomplete, illegible, or give the OA reason to believe that the application is invalid or fraudulent.

### **4.2.3 Time to Process Certificate Applications**

Certificate applications originating from individuals with an Illinois drivers license or State Id card may apply for their certificates online, in which case the certificate is normally issued within 1-5 minutes. Out of State certificate applicants must have an application form notarized and sent to the OA for processing. In this case, the certificate applications are processed within 48 hours of receipt.

### **4.3 ISSUANCE**

The PKIX Certificate request is digitally signed by the Subscriber using the newly generated signing key. Upon receipt of a valid request, the State CA automatically generates an encryption key pair and issues both a signature verification public key Certificate and an encryption public key Certificate for that Subscriber. Both Certificates and the decryption private key are returned to the Subscriber using the PKIX-CMP protocol. A self-signed root CA certificate is securely delivered to subscribers using PKIX-CMP during the certificate issuance process.

#### **4.3.1 CA Actions during Certificate Issuance**

Certificate requests are validated before certificate issuance. For in-State certificate requests that are processed online, the provided information is validated via a real-time call from the registration program to the Illinois Secretary of State driver's license database. If the information matches, a "yes" is returned. If the information does not match, a "no" is returned. No sensitive or private data is exchanged between the servers.

For out-of-State registration requests, the paper forms are validated before a certificate is created and authorization codes are sent to the subscriber.

#### **4.3.2 Notification to Subscriber of Certificate Issuance**

Once a certificate is issued to an individual, a "congratulations" message is displayed, indicating that the certificate has been created.

### **4.4 CERTIFICATE ACCEPTANCE**

As the PKIX operations are themselves secured and the two entities (Subscriber and CA) authenticated, successful completion of the PKIX request and response operations constitutes acceptance by the user of the resulting public key Certificates. By accepting the State Certificate, the Subscriber is warranting that all information and representations made by the Subscriber that are included in the State Certificate are true. Subscribers must either agree to the subscriber agreement online before creating a certificate, or must sign a copy of the certificate application form which contains the subscriber agreement. Either of these actions will indicate acceptance of the terms of the agreement.

Subscribers are bound by the subscriber agreement found at [http://www.illinois.gov/pki/pki\\_subscriber.cfm](http://www.illinois.gov/pki/pki_subscriber.cfm). Continued use of or reliance on a certificate after the 30 day waiting period as described in the State of Illinois Certificate Policy section 8.1.2 will be deemed acceptance of the modified terms.

#### **4.4.1 Conduct constituting certificate acceptance**

For the Illinois PKI, failure to object to the certificate or its contents constitutes acceptance of the certificate.

##### **4.4.1.1 *Multiple certificates caused by different registration methods***

Due to differences between the original certificate creation method and the web registration model, some recipients have received multiple certificates (i.e., same common name with a different serial number). This generally occurs when someone has undergone a face-to-face registration and activation codes have been generated, but the recipient has never activated their certificate. In this case, the old entries in the database and directory are removed. If the older certificate has been created, further checking is done to see if the certificate has been used for signing or encryption. If not, the older certificate is archived (since no key compromise is suspected). If the older certificate has been used, then the new certificate is archived.

#### **4.4.2 Publication of the Certificate by the CA**

Once created, the public portions of the certificate are posted in the repository. If the certificate is a “roaming” certificate, then the actual certificate (doubly-encrypted) is stored in the repository.

#### **4.4.3 Notification of Certificate Issuance by the CA to other entities**

For end-entity certificates, no stipulation. For CA certificates, any other cross-certified CA will be given notice of new cross-certifications.

### **4.5 KEY PAIR AND CERTIFICATE USAGE**

#### **4.5.1 Subscriber Private Key and Certificate Usage**

All certificate subscribers shall protect their private keys from access by other parties. Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

Certificates issued by the Illinois PKI can only be used for State/Governmental business. Private use of the certificate and associated software is prohibited.

#### **4.5.2 Relying Party Public key and Certificate Usage [Old §2.1.4]**

Relying parties will rely on a valid Certificate for purposes of verifying the digital signature only if prior to reliance, the Relying Party shall:

- (1) Agreed to be bound by the terms of this CP;

- (2) Verified the digital signature by reference to the public key in the Certificate; and
- (3) Referred to the most recent CRL.

Relying party understands that certificates are subject to revocation and such action shall not be reflected in the Certificate itself, but must be verified by consulting the most recent certificate revocation list.

Certificates issued by the Illinois PKI can only be used for State/Governmental business. Private use of the certificate and associated software is prohibited.

## **4.6 CERTIFICATE RENEWAL**

Digital certificates obtained through the State Internet registration process generate a (level 1) assurance level credential. If it becomes necessary to upgrade that certificate to a level 2 assurance level requires face-to-face verification, and the following steps will be followed:

Have the user/client fill out the following fields on the PKI Certificate Application form:

- Last Name
- First Name
- Middle Name
- Date of Birth
- Social Security Number
- Illinois Driver's license/State Identification card
- email address
- Requestor's signature
  - a. Perform the face-to-face verification as normal. Sign the form under "Local Registration Authority Signature".
  - b. Write "certificate upgrade" on the form in the bottom right corner.
  - c. Send the form to CMS as is currently done.

### **4.6.1 Circumstance for Certificate Renewal**

Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key.

The Illinois PKI doesn't support certificate renewal in accordance with the FPKI definition

### **4.6.2 Who may request Renewal**

Not applicable.



#### **4.6.3 Processing Certificate Renewal Requests**

Not applicable.

#### **4.6.4 Notification of new certificate issuance to Subscriber**

Not applicable.

#### **4.6.5 Conduct constituting acceptance of a Renewal certificate**

Not applicable.

#### **4.6.6 Publication of the Renewal certificate by the CA**

Not applicable.

#### **4.6.7 Notification of Certificate Issuance by the CA to other entities**

Not applicable.

### ***4.7 CERTIFICATE RE-KEY***

Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. This certificate becomes part of the certificate's key history. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.

Subscribers of Entity CAs will identify themselves for the purpose of re-keying as required in Section 3.3.1.

After certificate rekey, the old certificate (the one in key history) may or may not be revoked, but will not be further re-keyed, renewed, or modified.

#### **4.7.1 Circumstance for Certificate Re-key**

Certificates issued by the State CA (both device certificates and certificates for individuals) will be setup to automatically renewed. All encryption and digital signature key pairs will expire at the end of the Certificate validity period. Keys enter what is referred to as a transition period when they approach their lifetime end. The transition period is defined as the shorter of 100 days or 50% of the key lifecycle as defined in section 6.3.2 of this CPS.

#### **4.7.2 Who may request certification of a new public key**

Either cross-certified entities (when a currently recognized Principal CA has generated a new key pair and a valid and unexpired MOA exists between the Illinois Policy Authority) or end-entities may request a certificate re-key.

#### **4.7.3 Processing certificate Re-keying requests**

For both CAs and end-entities, the Illinois PKI Operational Authority shall identify and authenticate Principal CAs by either manual or automated means.

#### **4.7.4 Notification of new certificate issuance to Subscriber**

For CA certificates, the requesting CA shall be notified of the re-keying of a new certificate. For end-entities, no stipulation.

#### **4.7.5 Conduct constituting acceptance of a Re-keyed certificate**

For the Illinois PKI, failure to object to the certificate or its contents constitutes acceptance of the certificate.

#### **4.7.6 Publication of the Re-keyed certificate by the CA**

All CA and end-entity certificates will be published in the Illinois PKI repository.

#### **4.7.7 Notification of certificate issuance by the CA to other Entities**

The Illinois PKI Operational Authority shall inform any cross-certified entity of any new cross-certificate issuance or rekey.

For Entity CAs, no stipulation.

### **4.8 MODIFICATION**

Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, an Entity CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.

After certificate modification, the old certificate that resides in key history may or may not be revoked, but must not be further re-keyed, renewed, or modified.

#### **4.8.1 Circumstance for Certificate Modification**

A certificate may be modified in the case of an email address change, a distinguished name change, or any other change approved by the OA.

#### **4.8.2 Who may request Certificate Modification**

Either CAs or end-entities may request certificate modification.

#### **4.8.3 Processing Certificate Modification Requests**

If requested, the Illinois PKI Operational Authority will perform certificate modification at the direction of the FPKI PA providing the change does not impact the Illinois PKI. The Illinois PKI Operational Authority may also perform certificate modification at the request of the Entity CA for the following reasons:

- Modification of SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.
- Email address changes
- Distinguished name changes

The validity period associated with the new certificate must not extend beyond the period of any MOA.

For Entity CAs, proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued.

#### **4.8.4 Notification of new certificate issuance to Subscriber**

No stipulation.

#### **4.8.5 Conduct constituting acceptance of modified certificate**

For the Illinois PKI, failure to object to the certificate or its contents constitutes acceptance of the certificate.

#### **4.8.6 Publication of the modified certificate by the CA**

All updated certificates are published in the Illinois PKI repository.

#### **4.8.7 Notification of certificate issuance by the CA to other Entities**

Notification will be given to any cross-certified entity if another cross-certificate is modified. For end-entities, no stipulation..

### ***4.9 CERTIFICATE REVOCATION & SUSPENSION***

#### **4.9.1 Circumstance for Revocation**

A Certificate will be revoked when the Subscriber no longer wants or requires a certificate, or when the Public Key password, token or profile associated with the

certificate is compromised or suspected of being compromised. Certificates may also be revoked by the CA upon failure of the Subscriber to meet its obligations under this Policy or any other agreement, regulation, or law that may be in force. Subscribers will request revocation promptly following detection or suspicion of a compromise or any other event necessitating revocation. The RA or LRA may originate a certificate revocation if knowledge or suspicion of compromise is obtained. The rationale for such a revocation will be documented, signed by at least one of the CA personnel, and archived.

A Certificate holder's encryption and/or verification certificate will be revoked when the certificates are no longer trusted, for any reason. Some of the specific reasons for loss of trust in certificates include, but are not limited to:

- Compromise or suspected compromise of private keys and/or user passwords and profile;
- Failure of the subscriber to meet their obligations under this CP and CPS;
- Failure to prove continued ownership of the private keys;
- Request by the Subscriber;
- Receipt of a certified copy of subscriber's death certificate;
- When information on a certificate changes or becomes obsolete; or
- If the issuing CA determines that the Certificate was not properly issued in accordance with the Certificate Policy.

Agency staff may see indications that a particular certificate cannot be trusted through the course of conducting electronic transactions that involve a particular certificate; however, change in employment status with the agency is NOT by itself a justification for revocation of a certificate.

Revocation will be done in accordance with the procedures established by the Operational Authority as defined in Appendix A of this CPS.

#### **4.9.2 Who can request Revocation**

Revocation of an Individual's certificate will be requested by one of the following entities; the CA, RA or LRA for the Subscriber's organization, the sponsoring State agency, or by the Subscriber themselves.

#### **4.9.3 Procedure for Revocation Request**

If a PKI Administrator is initiating a revocation request, they login by providing the appropriate credentials to Entrust/RA and initiate a revocation request to Entrust/Authority™ for execution.

If an End Entity, who is the subject of the Certificate to be revoked, or one of the other individuals identified in section 5.2.1 of this CPS, is initiating the revocation request, the initial request is made off-line. If possible, the individual presents himself or herself in person along with a photo id card. If that is not possible (e.g. the Subscriber is on extended travel), an email request can be sent to the RA.

Upon receipt of a valid request, a PKI Administrator will login by providing the appropriate credentials to the Entrust/RA system and initiate a revocation request to Entrust/Security Manager™ for execution.

In all cases, a record is retained in the software audit trail of the online request and a paper record of any offline request is retained by the OA.

Revoked certificates (including the reason for revocation) will be included on all new publications of the CRL until the certificate expires.

If the subscriber whose certificate has been revoked feels the certificate has been revoked in error, the subscriber should contact the Policy Authority to schedule a hearing so that the matter may be resolved.

#### **4.9.4 Revocation Request Grace Period**

In the case of key compromise, suspected key compromise, or dismissal for cause, the revocation request should be placed within no more than 8 hours of the detection of the compromise or suspected compromise.

- Revocation requests for other revocation reasons must be placed within 48 hours of the change.
- Revocation requests will be processed within 18 hours from time of receipt by the RA.
- The State CA is not liable for any damages due to the failure of a Subscriber to meet these requirements for requesting revocation.

#### **4.9.5 Time within which CA must Process the Revocation Request**

The Illinois PKI will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance shall be processed before the following CRL is published. CRL's are automatically reissued after a revocation.

#### **4.9.6 Revocation Checking Requirements for Relying Parties**

CRL checking is done automatically by the CA software.

#### **4.9.7 CRL Issuance Frequency**

As a minimum, the State CA issues CRLs and ARLs on a 24-hour interval. The CRLs and ARLs are issued 7 days per week. On an exception basis, CRLs and ARLs may also be issued between these intervals (e.g. upon detection of a serious compromise situation or a certificate revocation).

#### **4.9.8 Maximum Latency of CRLs**

Each Certificate issued by the State CA includes the full DN of the CRL Distribution Point to be checked during the verification of the Certificate. Relying Parties, when working in an online mode, will check the current CRL, identified by the DN in the Certificate's CRL Distribution Points extension field, along with any other CRLs required in Certificate chain processing prior to trusting the Certificate.

When working in an offline mode, Relying Parties are not able to perform full CRL checking.

#### **4.9.9 On-line Revocation/Status Checking Availability**

Not supported.

#### **4.9.10 On-line Revocation Checking Requirements**

Not supported.

#### **4.9.11 Other Forms of Revocation Advertisements Available**

No stipulation.

##### **4.9.11.1 Checking requirements for other forms of revocation advertisements**

No stipulation.

#### **4.9.12 Special Requirements Related To Key Compromise**

In any key compromise situation, a report must be filed with the State PKI OA, or equivalent, indicating the circumstances under which the compromise occurred. If accidental, on the part of the Subscriber, no further action is required. Otherwise, the State PKI Administrator, or equivalent, will determine if a possible follow up investigation, potential action, or re-authentication is required in accordance with the existing IT Security Policy.

After revocation, the Subscriber cannot log onto the system and must be set up by a RA for key recovery.

#### **4.9.13 Circumstances for Suspension**

The Illinois PKI does not support the suspension of certificates.

#### **4.9.14 Who can Request Suspension**

No stipulation

#### **4.9.15 Procedure for Suspension Request**

No stipulation

#### **4.9.16 Limits on Suspension Period**

No stipulation

### ***4.10 CERTIFICATE STATUS SERVICES***

The Illinois PKI does not support Certificate Status Services.

#### **4.10.1 Operational Characteristics**

No stipulation.

#### **4.10.2 Service Availability**

No stipulation.

#### **4.10.3 Optional Features**

No stipulation.

### ***4.11 END OF SUBSCRIPTION***

No stipulation.

### ***4.12 KEY ESCROW & RECOVERY***

The Illinois PKI does not utilize key escrow.

#### **4.12.1 Key Escrow and Recovery Policy and Practices**

Not applicable.

#### **4.12.2 Session Key Encapsulation and Recovery Policy and Practices**

Not applicable.

## **5. FACILITY MANAGEMENT & OPERATIONS CONTROLS**

The focus of physical security controls is to minimize exposure from environmental hazards and malicious actions that could harm data or information, severely delay the timeliness of processing, or threaten the safety of personnel.

### **5.1 PHYSICAL CONTROLS**

Subscribers and Relying Parties will be made aware of any security practices they need to follow in the protection of their computers and cryptographic devices. The LRA is responsible for communicating these practices to all Subscribers and Relying Parties within its domain.

#### **5.1.1 Site Location & Construction**

All perimeter walls securing data processing and operations are slab-to-slab solid construction. All exterior perimeter windows are of a non-opening design to reduce the potential for undetected access through windows. The computer facility room has no windows.

#### **5.1.2 Physical Access**

The Entrust/Authority system is located in a locked facility to which only authorized State personnel have physical access with camera surveillance. The room containing the Entrust/Authority system is designated a security area, and appropriate controls are deployed to assure that no unauthorized personnel enter the room. Alarm systems are deployed to notify security personnel of violations. All visitors to the locked facility must be escorted by authorized personnel. A sign-in sheet is maintained which must be filled in by anyone entering/exiting the locked facility. Two factor authentication is required to enter the room housing the Illinois CA and Master Directory.

The data center is locked at all times and requires authorized access to allow entry. Successful and unsuccessful access attempts are recorded. In addition, all doors are equipped with audible warning devices that alert security personnel of unauthorized access/egress. With the 24 hour, 7-day operation that exists in the data center, the potential of undetected forced entry is minimal.

##### **5.1.2.1 Physical Access for CA Equipment**

- Access is limited to authorized personnel or escorted visitors.
- The data center has cameras to monitor and record activity.
- Two factor authentication is in place to restrict access to the CA.

##### **5.1.2.2 Physical Access for RA Equipment**

The RA and LRAs will implement at a minimum the following controls:



- The RA computers will have the password protected screen saver feature enabled, and computers will not be left unattended when the Private Key is in the unlocked state (i.e. when the password has been entered);
- The RA and LA will physically protect any password that allows access to keys. Passwords will be protected at the level of assurance associated with the certificate and when written down, will be stored in a locked file cabinet or container accessible only to the RA or LRA;
- If a private key is stored encrypted on a diskette or other unsecured medium, such diskette or other medium will be stored in a locked file cabinet or container when not in use; and
- LRAs will not leave their computers unattended when the Private Key is in an unlocked state (i.e., when the password has been entered).
- Any RA or LRA computer that contains private keys encrypted on a hard drive must be secured.

#### **5.1.2.3 *Physical Access for CSS Equipment***

No Stipulation.

#### **5.1.2.4 *Physical Security Controls for Subscribers***

Each Subscriber must physically protect any password that allows entry into the Subscriber's CA Client application. If a password must be written down, it should be securely stored such that only the Subscriber has access to it. Subscribers must not leave their computers unattended when the Private Key is in an unlocked state (i.e., when the password has been entered).

#### **5.1.3 Power and Air Conditioning**

The State data center facility is fully equipped with uninterrupted power (including air conditioning). Routine and frequent inspections of all emergency systems are made to assure adequate operation.

#### **5.1.4 Water Exposures**

The State data center facility is fully equipped with protection from water damage. Routine and frequent inspections of all emergency systems are made to assure adequate operation.

#### **5.1.5 Fire Prevention & Protection**

The State data center facility is fully equipped with fire protection and suppression equipment. Routine and frequent inspections of all emergency systems are made to assure adequate operation.

### **5.1.6 Media Storage**

Archived records will be transferred to separate physical media that is external to the CA host system and primary CA application installation.

### **5.1.7 Waste Disposal**

Any information deemed to be of a sensitive nature and not required as a PKI archival document will be shredded.

### **5.1.8 Off-Site backup**

Data backups will be taken weekly.

- Weekly backups will be kept for three months and will be stored securely on site.
- Each week one set of backup tapes will be taken to the local area off site vault.
- Each quarter a complete set of system tapes will be taken to the off-site out of regions storage location in St. Louis. (This interval is subject to change as system demands grow)
- Audit logs will be removed from the system as space requirements dictate. These logs will be backed up on special tapes and archived.
- Other system backups will be taken before and after any major system changes.

## **5.2 PROCEDURAL CONTROLS**

### **5.2.1 Trusted Roles**

The State CA is represented by the Entrust/Security Manager software. The main administrative interfaces to Entrust/Security Manager are the Entrust/Security Manager Administration tool and Master Control. These interfaces are used by PKI entities with special privileges, to perform the CA and RA functions in the State PKI. These roles and associated privileges are described below:

At the State, there are three Master Users. Their PKI Master User passwords are documented and stored in a safe approved by the State OA. The Master Users have authority to:

- Maintain Entrust/Security Manager services (consisting of Administration Services, Key Management Services, and Directory Services) plus the Entrust/Authority database.
- Recover Security Administrator and Security Administrator Backup in the event they have forgotten their passwords.
- Recover the Entrust Administration services, in the event its profile becomes damaged.
- Backup, re-encrypt and restore from backup as necessary, the Entrust Manager database.

In the Entrust context, the State personnel who specify the State CA's security policies are Entrust Security Administrators. The Entrust Security Administrator created during the installation of the Entrust Authority is the 'First Officer'. The First Officer, drawing from selected State personnel, creates additional Entrust Security Administrators. The main role of the Security Administrators is to set and administer the State's security policy as it applies to all PKI Subscribers. Security Administrators use Entrust/Registration Authority as their interface to Entrust/Security Manager and have the following privileges:

- Set the security policy for the CA, and alter it,
- Add, delete and deactivate other Security Administrators, Local Registration Authorities, Directory Administrators and Subscribers,
- Authorize sensitive operations, such as adding and deleting Security Administrators and Certificate Authority Administrators,
- Process audit logs and
- All Certificate Authority Administrator privileges.

In the Entrust context, the State personnel and any others who are RA's have Administrator privileges. These are:

- Add, delete and suspend Subscribers,
- Manage key recovery for Subscribers,
- Revoke Subscriber Certificates, and
- Change Subscriber DNs.

State staff performs the role of System Administrator and has root access to the CA operating system. The Operation Authority will perform routine self-assessments of security controls.

In the event that the PKI disaster recovery plan is activated, at least 1 master user or OA member will be present during the recovery process. Sensitive material, such as the CA private signing key, will remain in the possession of one of these persons at all times until it's activation at the disaster recovery site.

#### **5.2.1.1 Administrator**

##### ***System Administrator***

The System administrator role is responsible for:

- Installation, configuration, and maintenance of the CA hardware and software;
- Establishing and maintaining CA system accounts;

System Administrators do not issue certificates to subscribers.

The System Administrator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

The System Administrator role is also known as the Operator role.

### ***CA Administrator***

The CA (security) Administrator role is responsible for:

- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.
- CA Administrators can issue certificates to subscribers.

The CA Administrator role is responsible for the overall maintenance of the running and operation of the CA as it pertains to certificate creation and usage.

### ***Directory Administrator***

The Directory Administrator is responsible for the availability and maintenance of the PKI repository, including the following functions:

- Creating and maintaining searchbases
- Creating and maintaining shadow agreements
- Monitoring the performance of the directory

#### ***5.2.1.2 First Officer***

The First Officer role is responsible for issuing certificates, that is:

- Registering new subscribers and requesting the issuance of certificates;
- Verifying the identity of subscribers and accuracy of information included in certificates;
- Approving and executing the issuance of certificates, and;
- Requesting, approving and executing the revocation of certificates.

#### **5.2.1.3 Auditor**

No stipulation.

#### **5.2.1.4 Master User**

Master Users perform functions relating to CA “master commands”, Examples include, but are not limited to:

- resetting the First Officer’s password
- recovering the Informix database
- Setting CA system parameters using the Master shell

Some master user commands require multiple master users to perform.

#### **5.2.1.5 Local Registration Authority**

Local Registration Authorities are authorized to perform face-to-face verifications for identification necessary for certificate issuance/upgrade. They also serve as the main point of contact for operational matters for the OA.

#### **5.2.1.6 Bulk Operations Administrator**

This role can process bulk files for certificate creation (normally out-of-State registrations) only. This role has no administrative authority.

### **5.2.2 Number of Persons Required per Task**

All Security Administrators operations need one Security Administrator authorization. Certain functions, such as activation of the CA Private Key, will be protected by multi-person controls (see Section 5.2.2 of the CP). In the State PKI the following operations need two Master User authorizations:

- adding and deleting Security Administrators;
- Changing a Security Administrator’s password;
- CA Master Key updates.

### **5.2.3 Identification and Authentication for Each Role**

Refer to section 3.2.3 of this CPS for identification and authentication procedures for individuals filling the Trusted Roles in the State PKI.

### **5.2.4 Separation of Roles**

Individual personnel shall be specifically designated to the seven roles defined in Section 5.2.1 above. Individuals may assume only one of the Administrator and Auditor roles. Individuals designated as Officer or Administrator may also

assume the System Administrator/Operator role. An auditor may not assume any other role. The CA and RA software and hardware shall identify and authenticate its users and shall enforce these roles. This shall not preclude the overlapping of roles for training and/or backup purposes.

### **5.3 PERSONNEL CONTROLS**

Three individuals will be assigned Entrust Master User responsibility.

At least two individuals will be assigned Security Administrator privileges.

Each participating State Agency, and other entities as determined by the State PA, may nominate one or more individuals to serve as LRAs for the organization. LRA privileges will be granted at the discretion of the RA. Prospective LRAs will return a completed LRA application form and a signed LRA agreement (wet signature or digitally signed) to the RA and will submit themselves to a State Police criminal background check. Should the background check reveal that the applicant has been convicted of or committed a crime of moral turpitude; the applicant will be subject to disqualification at the discretion of the RA. If an LRA is formally accused of a crime other than a petty traffic offense (for which the fine does not exceed \$100.) he/she must within three days of being charged notify the RA. The RA will periodically conduct random background checks of LRAs, to assure compliance with the ongoing reporting requirements of this section.

LRA privileges may be denied, suspended, or revoked at the discretion of the RA. Reasonable notice and opportunity for hearing will be provided, as warranted by the specific circumstances. Hearings will be conducted by the PA, which will have the authority to uphold or overrule actions by the RA denying, suspending or revoking LRA privileges. The RA may deny, suspend, or revoke LRA privileges for good cause shown, including but not limited to:

- Commission or conviction of a criminal offense involving moral turpitude;
- Failure to cooperate fully in any investigation by the RA or PA;
- Failure to comply with the CP and the CPS;
- Separation from, or reassignment within the sponsoring governmental entity;
- Refusal or inability to diligently complete the obligations of an LRA.

All individuals fulfilling Trusted Roles will be full-time State employees.

#### **5.3.1 Background, Qualifications, Experience, & Security Clearance Requirements**

CA and RA personnel will:

- Be appointed by the PA;
- Be a State employee or other authorized individual not subject to frequent re-assignment or extended periods of absence.

### **5.3.2 Background Check Procedures**

Entity CA personnel shall submit to and pass an Illinois State Police background investigation which covers convictions incurred by the individual from the age of 17 on. If the background check reveals that the applicant has been convicted of a criminal offense, the applicant is subject to disqualification at the discretion of CMS, with the advice of the PA.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

**Initial Qualification:** All Trusted roles must undergo identity checking consistent with obtaining a level 3 certificate (fingerprinting with Illinois State Police background check). Each participating State agency, and other entities as determined by CMS, with the advice of the PA, may nominate one or more individuals to serve as LRAs for that entity. Prospective LRAs must return a completed LRA application form and a signed LRA agreement (wet signature or digitally signed) to CMS. Applicant individuals must submit to a Department of State Police criminal history background check. If the background check reveals that the applicant has been convicted of a criminal offense, the applicant is subject to disqualification at the discretion of CMS, with the advice of the PA.

**Ongoing Qualification:** If a qualified LRA is formally accused of a criminal offense, the applicant must, within 3 days after being charged, notify CMS, which will notify the PA. CMS will periodically conduct random criminal history background checks of LRAs to assure compliance with this policy.

**Disqualification.** LRA privileges may be denied, suspended, or revoked at the discretion of CMS, with the advice of the PA. Reasonable notice and opportunity for hearing under Section 105.60 of the Illinois Administrative rules shall be provided. Grounds for denial, suspension or revocation of LRA privileges include, but are not limited to:

- Conviction of a criminal offense.
- Failure to cooperate fully in any investigation by CMS.
- Failure to comply with the Act, this Part, the CP and the CPS.
- Separation from, or reassignment within, the sponsoring entity.
- Refusal or inability to diligently complete the obligations of an LRA.

### **5.3.3 Training Requirements**

CA and RA personnel will receive proper (informal, formal, or on-the-job training) and continuous training in relation to their assigned duties. Documentation will

be maintained identifying all personnel receiving training and the level of training completed.

#### **5.3.4 Retraining Frequency & Requirements**

All Operational Authority members will receive proper and continuous training in relation to their assigned duties throughout the calendar year. Documentation will be maintained identifying all personnel receiving training and the level of training completed.

#### **5.3.5 Job Rotation Frequency & Sequence**

No stipulation.

#### **5.3.6 Sanctions for Unauthorized Actions**

Any member of the Operational Authority performing unauthorized functions will have their role changed so that rights to administrative functions are removed. Additionally, disciplinary action may be pursued depending on the severity of the action.

#### **5.3.7 Independent Contractor Requirements**

All independent contractors required for on-site support during the in-service phase of the CA will be escorted.

#### **5.3.8 Documentation Supplied To Personnel**

LRAs will:

- Read and understand the CMS document entitled “Local Registration Authority Administrative Rules.”
- Read and understand the CMS document entitled “Local Registration Authority Guidelines for Registration.”

### **5.4 *AUDIT LOGGING PROCEDURES***

#### **5.4.1 Types of Events Recorded**

All significant security events on Entrust/Authority™ will be automatically time stamped and recorded in audit trail files. These include such events as:

- Successful and failed attempts to initialize end-users, remove, enable, disable, update, and recover users, their keys and Certificates;
- Successful and failed attempts to create, remove, login as, set, reset and change passwords of, revoke privileges of, create update and recover keys and Certificates for Entrust/Authority™ and Local Registration Authorities;
- Failed interactions with the Directory including and failed connection attempts, read and write operations by Entrust/Authority™;



- All events related to Certificate revocation, security policy modification and validation, Entrust/Authority™ software startup and stop, database backup, Certificate and Certificate chain validation, attribute Certificate management, user upgrade, DN change, database and audit trail management, Certificate life-cycle management and other miscellaneous events.
- Some events, such as adding/removing items from safes, escorting personnel into the secured room, etc, are not captured on automated audit logs. All such events will be recorded in logbooks, on paper forms, or some other physical mechanism.

#### **5.4.2 Frequency of Processing Log**

The audit trail is reviewed for policy violations or other significant events at least once per week. Any violations or significant events are then reported to CA personnel. Such reviews will involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the log. Examples of irregularities include discontinuities in the logs, loss of audit data, or audit alarm records. Actions taken as a result of these reviews shall be documented. Audit alarms will be documented using a digitally signed audit report which records any alarms and includes comments as to what occurred and if further action is required. This form for audit alarms will generally be produced on a weekly basis.

For the Illinois CA, the Illinois Operational Authority will explain all significant events in an audit log summary.

#### **5.4.3 Retention Period for Audit Logs**

The audit trails are retained for a minimum of five years under normal operation.

#### **5.4.4 Protection of Audit Logs**

The audit trail is stored in regular operating system flat files. Each audit trail file consists of an audit header, which contains information about the audits in the file and list of events. A Message Authentication Code (MAC) is created for each of the audit events and the audit header. Each audit trail file has a different audit key used to generate the MAC. The Entrust master key for the State CA is used to protect the audit key, which is stored in the audit header.

The audit trail can be spread across many files. A new audit trail file is created when the current audit trail file reaches a preset size of 100 Kbytes or the Entrust master key is updated.

Security Administrators, Certificate Authority Administrators, and Directory Registration Authorities are capable of viewing and processing audit trail files.

#### **5.4.5 Audit Log Backup Procedures**

Audit trail files are archived by the system administrator on a weekly basis. All files including the latest audit trail file are moved to magnetic tapes and stored in a secure offsite archive facility.

#### **5.4.6 Audit Collection System (internal vs. external)**

The audit trail accumulation system is internal to Entrust/Authority™ software system.

#### **5.4.7 Notification to Event-Causing Subject**

State CA personnel causing audit events should receive notification, as appropriate, via the Entrust/RA interface.

Users causing audit events receive notification, as appropriate, via the Entrust desktop software interface. Such notifications are conveyed from Entrust/Security Manager™ to Entrust desktop software using the PKIX protocol.

#### **5.4.8 Vulnerability Assessments**

The State of Illinois Operational Authority will review system and application logs in accordance with section 5.4.2. This assessment activity is the internal audit activity related to the Illinois PKI. This activity in conjunction with the external compliance audit satisfies the auditing requirements for a Medium assurance CA.

### **5.5 RECORDS ARCHIVE**

The audit trail files and Entrust/Authority™ database are both archived.

#### **5.5.1 Types of Events Archived**

The types of events recorded in the audit trail files are described in this CPS.

The types of events recorded in the Entrust/Authority™ database include:

- Creation of the CA signing key pair;
- Addition and removal of end users from the system;
- Changes to the encryption key pair history and verification public key history for all users, including Certificate issuance and revocation events;
- Changes to the DN of end users;
- Changes of Administrator Role privileges;
- Changes to some aspects of policy such as Certificate validity period; and
- Creation and revocation of cross-Certificates.

### **5.5.2 Retention Period for Archive**

Archive of the Entrust/Authority™ database is retained for at least 30 years. Archives of audit trail files are retained for at least five years.

### **5.5.3 Protection of Archive**

The Entrust/Security Manager™ database is encrypted and protected by master keys. Integrity of the audit trail is as described in this CPS.

The archive media is protected by physical security in that it is retained in a restricted access facility to which only Authorized Operations Personnel and Security Administrators acting in tandem have access. Access to the archive media is processed according to CMS's existing policies, the Vault Access List within the CMS Internal Security Policy, and in accordance with the "State Records Act 5ILCS 160/1 et seq."

The archive data will be digitally signed by the State's CA. This will provide an integrity check that can be used to verify that the data has not been modified.

No unauthorized user will be permitted to write to, modify, or delete the archive data.

### **5.5.4 Archive Backup Procedures**

Archive files are backed up as they are created. Originals are stored on-site and housed with the Entrust/Security Manager™ system.

#### **5.5.4.1 Items to be archived**

All sensitive events, lists, certificates, keys, records, reports, and agreements (cross-certification and others) will be archived. In the case where an electronic version does not exist, a duplicate of the paper version will be created and archived.

### **5.5.5 Requirements for Time-Stamping of Records**

Time and date stamping of audit logs is an inherent function of the Entrust management software, therefore this requirement is automatically invoked at system startup.

### **5.5.6 Archive Collection System (internal or external)**

The archive collection system (backup facility) for the Entrust/Security Manager™ database is internal to the Entrust/Security Manager™ system.

The archive collection system (backup facility) for the audit trail files is described in section 5.5.4 of the CP.

The archiving of both data stores onto separate media and secure storage of that media is external from the Entrust/Security Manager™ system.

### **5.5.7 Procedures to Obtain & Verify Archive Information**

CA archive material is created internally by the Entrust software and is copied onto tapes via scheduled jobs on the AIX system. These tapes are labeled as to their contents and stored in-house until it is time for them to be archived. When this information needs to be taken to the archive site, the tapes and any other material to be archived are transferred to a locking transport bag. Two trusted roles are then required to deliver the archive material to the appropriate archive site. The archive material is then stored securely in either a safe or a vault, depending on the archive site.

## **5.6 KEY CHANGEOVER**

The PKI Security Administrator and Certificate Authority Administrator Certificates are set up for automatic key update. As such, both the encryption and digital signature key pairs are automatically updated prior to expiry.

### **5.6.1 Recovery at Subscriber Request**

When a subscriber requests that their own profile be recovered due to the subscriber no longer being able to access his/her private keys due to the password being lost or the electronic file being corrupted, the subscriber must provide proof of identity through secured shared secrets or other authentication prior to recovery of the Subscriber's profile. The recovery will then be performed using the following procedures:

- If the subscriber is in possession of an Illinois driver's license or identification card, they will perform a self-recovery by accessing the web site [www.illinois.gov/pki](http://www.illinois.gov/pki) and choosing the "forgot password" link.
- If the subscriber does not possess an Illinois driver's license or identification card, the user must contact the Operational Authority, who will verify their identity against the paper application forms. Once the subscriber's identification has been verified, the subscriber will be manually put into a key recovery state by an OA member. One of the authentication codes will be provided to the user at the time of the identification verification, and the other will be emailed to the subscriber, along with a url to visit to complete the key recovery.

### **5.6.2 Involuntary Recovery at State Agency Request**

A State Agency may request involuntary recovery of a Subscriber's private encryption keys that person is or has recently been employed by the State of Illinois, the Agency has reason to believe that data necessary to agency operations has been encrypted using the Subscriber's keys, and the Agency is unable to contact the Subscriber or the Subscriber is unable or unwilling to decrypt the data.

The Agency's request will be made in writing to the PA, describing why the Subscriber's private encryption key is necessary to Agency operations and specifying what use will be made of the key. The request will be signed by the Director of the Agency. The Subscriber's keys will not be recovered until said request is reviewed by the PA or those designated by the PA to review such requests.

Prior to recovering the Subscriber's profile, the OA will alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate will be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA will sign for receipt of the profile, will supervise all Agency use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked following the procedures in Section 4.4 "Certificate Suspension and Revocation".

A Subscriber whose profile has been revoked as part of an involuntary recovery must follow the procedures described in Section 3.3.1 "Rekey after Revocation" to be re-authenticated and issued a new Certificate.

### **5.6.3 Involuntary Recovery by Court Order**

The PA and OA will comply with all official, authorized, and verified court orders to recover a Subscriber's keys.

- Prior to recovering the Subscriber's profile, the CA will alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate will be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA will sign for receipt of the profile, will supervise all Agency use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked following the procedures in Section 4.9 "Certificate Suspension and Revocation".
- A Subscriber whose profile has been revoked as part of an involuntary recovery must follow the procedures described in Section 3.3.2 to be re-authenticated and issued a new Certificate.

## **5.7 COMPROMISE & DISASTER RECOVERY**

In the event of a disaster or serious compromise, the following steps, as a minimum, are taken to recover a secure environment:

- All user passwords are changed for Security Administrators and Certificate Authority Administrators;
- Depending on the nature of the disaster, some or all user Certificates are revoked;
- The Directory data, encryption Certificates and CRLs, are restored if the Directory becomes unusable and must be restored from backup or

if the Directory is suspected to be corrupt. Once the Directory Administrator has restored the Directory from backup, a Master User will restore the data to the Directory from the Master Control system;

- Should a Security Administrator profile need recovery, the backup Security Administrator can recover it. If neither of the Security Administrators have valid Security Administrator privileges in existence to recover a Security Administrator profile, a Master User will recover the profile through the Master Control system.

#### **5.7.1 Incident and Compromise Handling Procedures**

No stipulation.

#### **5.7.2 Computing Resources, Software, and/Or Data Are Corrupted**

All operations will be covered by a Business Continuity Plan that provides for a smooth transition to alternate equipment and/or facilities in case of equipment failure or facility damage. Additionally, there will be a separate disaster recovery plan for the Illinois PKI.

All software and data are backed up daily in multi-generation backups that can be used to restore corrupted software or data or to recover from a hardware failure.

#### **5.7.3 Entity (CA) Private Key Compromise Procedures**

In the event that it becomes necessary to revoke the State CA Certificate, the following actions will be taken:

- The status of all Certificates in the State Certificate Repository that were issued by the affected CA key will immediately be changed to "Revoked";
- All affected Subscribers will be notified via both e-mail and U.S. mail that their Certificates have been revoked, what necessitated the revocation, and how to register for replacement Certificates.
- All other CAs and Relying Parties will be notified so that they can remove the trust associated with the revoked the State CA Certificate in their systems.

#### **5.7.4 Business Continuity Capabilities after a Disaster**

All operations will be covered by a Business Continuity Plan that provides for a smooth transition to alternate equipment and/or facilities in case of equipment failure or facility damage.

#### **5.7.5 System backup procedures**

- Backups of the Informix database, vital infrastructure files, and the LDAP directory will be taken weekly.

- MakeSysB (bootable images) backups will be taken weekly. These backups will be on separate tapes than those used for the database, directory, and infrastructure backups.
- Weekly backups will be kept for three months and will be stored securely on site.
- Each week one set of backup tapes will be taken to the off site vault.
- Each quarter a complete system backup will be taken to the off-site storage location in St. Louis. (This interval is subject to change as system demands grow)
- Audit logs will be removed from the system as space requirements dictate. These logs will be backed up on special tapes and archived.
- Other system backups will be taken before and after any major system changes.

## **5.8 CA & RA TERMINATION**

In the event that the State CA ceases operation or is otherwise terminated:

- All Subscribers, sponsoring organizations, and Relying Parties must be promptly notified of the cessation;
- All CAs with which cross-certification agreements are current at the time of cessation will be informed so that cross-Certificates to the State CA may be revoked;
- All State Certificates issued by the State CA will be revoked no later than the time of cessation; and
- All current and archived State identity proofing, Certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data will be archived according to the State data archive policy.

Notification methods could include but are not be limited to web site notification, mass email, media advertisements, etc.

## **6. TECHNICAL SECURITY CONTROLS**

The State will implement comprehensive technical controls for the State PKI, will ensure that the system is continuously operated within the approved security parameters and that all required technical controls remain in place and properly configured.

### **6.1 KEY PAIR GENERATION & INSTALLATION**

Most PKI users will have the digital signature key pair generated in software. Some Entrust users may have hardware tokens which generate this key pair. The keys generated by the State CA are generated in software in Entrust/Security Manager™ with the exception of the CA private signing key, which is generated on the Luna CA 3 token.

#### **6.1.1 Key Pair Generation**

The CA signing key pair is created during the initial start up of the Entrust/Master Control application and is protected by the CA master key.

The software key generation process is designed to comply with FIPS 140-1 level 1. With hardware tokens, the generation process may be compliant with higher levels of FIPS validation.

For all the State PKI key pairs the encryption key pair and the corresponding encryption Certificate are created by Entrust/Security Manager™. The digital signature key pair is generated by the client software or in some cases by a hardware token. Keys generated by software may be stored in a software file or on a hardware token. These products contain at least a FIPS 140-1 approved cryptographic module.

##### **6.1.1.1 CA Key Pair Generation**

The Illinois PKI was created via a root key ceremony conducted on January 17-18, 2001. This ceremony was audited and witnessed by Deloitte and Touche and the State Auditor General's office. Any future CA key pair generations must adhere to the following requirements:

- The key generation ceremony must be audited.
- The key generation ceremony must be conducted via a written script containing all of the commands necessary to achieve the key generation/update. If automated scripts are created, the contents of these scripts must be printed as well.
- The key generation must first be conducted on a test environment.



- Before the key generation is performed on the production environment, a “dry run” must be conducted on a test system and audited to ensure the validity of the script.
- The activities of the ceremony must be documented afterwards.
- Copies of the scripts must be maintained.

#### **6.1.1.2 Subscriber Key Pair Generation**

Subscriber key pairs may be generated in various ways. End-entity subscribers who have an Illinois driver’s license or ID card may generate their initial (Level 1) keys using the online registration system provided. This creates a roaming certificate which stores the credentials and key pairs in the Illinois PKI repository (doubly-encrypted).

Out of state end-entity subscribers must fill out a registration form and present it (plus appropriate forms of identification) to a notary public, who must sign and stamp the application. This form is then sent to the OA, who then generates two activation codes. One code is provided via email, and the other is provided out-of-band via a printed mailer. Instructions are on the mailer to logon to a particular web site to complete the registration and generate the certificate and the key pairs.

Device certificates and some special end-entity certificates are generated through the CA interface. This is done by OA personnel only. Device certificates require a form to be completed and signed by the entity LRA before they are created.

#### **6.1.2 Private Key Delivery to Subscriber**

The private decryption key is provided securely to the user via PKIX protocol exchange between Entrust/Security Manager™ and Entrust desktop software or between Entrust/Security Manager™ and the user’s hardware token. The authorization code is used to derive a MAC key, which is then used to provide authentication and integrity protection on the session. For the digital signature key pair, as the key pair is generated by the user, no delivery of the private key is required.

#### **6.1.3 Public Key Delivery to Certificate Issuer**

The encryption key pair is created by Entrust/ Security Manager™, and a copy of the public encryption key is placed in the Directory and delivery of the encryption public key to the Certificate issuer is required. The signature verification public key is delivered securely to Entrust/ Security Manager™ using the PKIX protocol.

#### **6.1.4 CA Public Key Delivery to Relying Parties**

The CA verification public key is delivered in a CA Certificate to users using the PKIX protocol. Authenticity and integrity protection is based on a MAC key derived from the authorization code.

#### **6.1.5 Key Sizes**

The State CA Security Administrator sets the following encryption key sizes:

Entrust user signing key pairs use the Rivest-Shimmar-Adleman (RSA) with Secure Hashing Algorithm-1 (SHA-1).

A minimum length of 1024 bits will be used for all key pairs. Support for optional key lengths of 2048 bits will be provided.

- Entrust user signing key pairs are 1024 RSA.
- Entrust user encryption key pairs are 1024 RSA.
- The State CA signing key pair is 2048 RSA.
- PKIX session keys are CAST-128.

#### **6.1.6 Public Key Parameters Generation and Quality Checking**

These parameters are inherent with the commercial off the shelf software implemented by the Illinois PKI.

#### **6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)**

Certificates issued by the State CA contain the key Usage Certificate extension restricting the purpose to which the Certificate can be applied.

- The digital signature key pair is used to provide authentication, integrity and support for non-repudiation services.
- The encryption key pair is used to protect a symmetric key used to encrypt data, and as such provides confidentiality services.
- The State CA signing key is used to sign Certificates, CRLs and ARLs issued by that CA.
- The PKIX session keys are used to provide secure communications for key management operations.

### **6.2 PRIVATE KEY PROTECTION & CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS**

#### **6.2.1 Cryptographic Module Standards & Controls**

The cryptographic module used by Entrust software to generate keys is designed to comply with FIPS 140-1 level 3. Some users have hardware tokens, which generate keys, and these may comply with higher levels of FIPS validation.

### **6.2.2 Private Key Multi-Person Control**

As described in section 5.2.2 of this CPS, a minimum of two-person control is required for some CA operations.

Other actions require one-person control.

### **6.2.3 Private Key Escrow**

Escrow of private keys by an external third party is not performed.

#### **6.2.3.1 *Escrow of Illinois CA private signature key***

The Illinois PKI does not utilize key escrow.

#### **6.2.3.2 *Escrow of Illinois CA encryption keys***

The Illinois PKI does not utilize key escrow.

#### **6.2.3.3 *Escrow of Subscriber private signature keys***

The Illinois PKI does not utilize key escrow.

#### **6.2.3.4 *Escrow of Subscriber private encryption and dual use keys***

The Illinois PKI does not utilize key escrow.

### **6.2.4 Private Key Backup [Old §6.2.4]**

CA private keys and user encryption private keys are backed up in the Entrust/Security Manager™ database. The user's private signing key is never backed up at Entrust/Security Manager™ in order to provide support for non-repudiation services. However, a user who makes a copy of their software profile essentially has an encrypted backup of their signing key. The Entrust/Security Manager™ database is encrypted and its integrity is protected by Entrust master keys. The CA signing key is encrypted and its integrity protected by the CA master keys. The CA signing Key is generated and stored on the Luna CA 3 token. The only backups of the CA Signing Key are maintained on additional Chrysalis Tokens.

#### **6.2.4.1 *Backup of Illinois CA Private Signature Key***

The Illinois PKI utilizes a clustered server approach utilizing HACMP to control the failover. Therefore, there are two CA signing key tokens present on the production system. Backups of both of these tokens are stored off-site.

#### **6.2.4.2 *Backup of subscriber private signature key***

For roaming certificates, backup of the private signing keys is done when the repository is backed up. This provides no security threat, since the profile in the repository is doubly-encrypted.

Non-roaming certificates are controlled by the subscribers, and are therefore out of the control of the Illinois PKI.

#### **6.2.4.3 Backup of Subscriber Key Management Private Keys**

For roaming certificates, backup of the private signing keys is done when the repository is backed up. This provides no security threat, since the profile in the repository is doubly-encrypted.

Non-roaming certificates are controlled by the subscribers, and are therefore out of the control of the Illinois PKI.

#### **6.2.4.4 Backup of CSS Private Key**

Not Applicable.

### **6.2.5 Private Key Archival**

The encryption key pair history for all users, including a complete history of all decryption private keys is stored encrypted in the Entrust/Authority™ database.

The Entrust/Authority™ database is backed up at a minimum on a daily basis.

Recovery of information from the Entrust/Security Manager™ database can be done by members of the Operational Authority.

### **6.2.6 Private Key Transfer into or from a Cryptographic Module [Old §6.2.6]**

CA signing private keys are generated and stored on the chrysalis token and most Subscriber signing private keys are generated in software, within the cryptographic module. In the case of hardware tokens, the token may or may not produce the private signing key at the end-entity. If the hardware token is a storage only device, the private signing key is generated in software and injected onto the device encrypted. Subject End Entity decryption private keys come from Entrust/Security Manager™, in an encrypted format, and are entered into the cryptographic module encrypted. In all cases, private keys are stored encrypted in the cryptographic module. In both the software and hardware token cases, they are decrypted only at the time at which they are actually being used.

For both software and hardware token cases, private keys are activated at the time the subject login to the relevant Entrust component occurs (e.g. Entrust/Entelligence/ESP for subject end-entities, Entrust/Security Manager™ for CAs).

### **6.2.7 Private Key Storage on Cryptographic Module**

A cryptographic module will associate a cryptographic key stored with in the module with the correct entity to which the key is assigned. According to documentation on the Safenet internet site, “4Mb of battery-backed secure key storage is available to safely store and maintain the integrity of symmetric cipher keys, asymmetric keys, certificates, and sensitive data. The battery provides back-up power to the tamper-sensing electronics when no system power is available. Any detected tamper event, including removing the battery from the HSM, or the HSM from the PCI bus slot, will immediately activate key memory erasure.”

### **6.2.8 Method of Activating Private Keys**

Private keys will be activated by authenticating the Subscriber to the Luna cryptographic module. Acceptable means of authentication include pass-phrases, PINS, and biometrics.

### **6.2.9 Methods of Deactivating Private Keys**

The private keys remain active for the period of login. The login period is ended either by the subject logging out from the Entrust application or automatically after a preset period of time configured in Entrust/Security Manager™. The preset timer is controlled from Entrust/Security Manager™ by the Security Administrator.

### **6.2.10 Method of Destroying Private Keys**

All sensitive keys in memory are overwritten with zeros when no longer used. Permanent destruction of private keys is achieved with secure delete operations. The CA private key can also be destroyed using the “zeroize” command for the Luna token.

### **6.2.11 Cryptographic Module Rating**

The State of Illinois Root CA will use only tokens and token readers that have been certified by the National Institute of Standards and Technology program standard for cryptography as FIPS 140-1 level 3 certified.

## **6.3 OTHER ASPECTS OF KEY MANAGEMENT**

### **6.3.1 Public Key Archival**

The user encryption public key Certificates and verification public key Certificates are backed up in the Entrust/Authority™ database. The complete encryption key pair history and verification public key history for all users, including history of

status changes such as revocation date and reason, are archived in this database.

All public keys will be archived in accordance with the records archival practices described in section 5.5 (and its sub-sections) of this CPS.

### **6.3.2 Certificate Operational Periods/Key Usage Periods**

The CA signing key lifetime is set to twenty years.

Subscriber Certificates issued by the State will have a validity period of three (3) years. Subscribers may use their private keys only during the validity period of the corresponding Certificate. Additionally, they may not use their private keys before they have accepted the Certificate from the State CA (i.e., during the period between key generation and Certificate acceptance). Public keys on expired Certificates may be used to validate signatures on objects that were signed during the validity period of the Certificate.

The key lifetimes for certificates are:

- Encryption public key: 36 months (3 years)
- Verification public key: 36 months (3 years)
- Signing private key: 25 months (70% of verification public key lifetime)

The signing private key lifetime must be less than or equal to the corresponding verification public key expiration date.

## **6.4 ACTIVATION DATA**

### **6.4.1 Activation Data Generation & Installation**

Passwords are required by all entities logging on to Entrust components. Entrust applies a stringent set of rules to each password to ensure it is secure. Some of the rules on password selection are:

- It must have at least eight characters;
- It must have at least one upper-case letter or digit;
- It must have at least one lower-case letter;
- It must not contain many occurrences of the same character;
- It must not be the same as the entity's profile name;
- It must not contain a long substring of the entity's profile name;
- Passwords for RA's and LRA's will expire after 5 weeks;
- Passwords for subscribers will expire after 52 weeks.

### **6.4.2 Activation Data Protection**

Extra steps are taken to protect passwords. Once chosen, the password is put through numerous hashing iterations, producing a password token. Only the password token is stored in a user's client profile. Original passwords are never stored.

### **6.4.3 Other Aspects of Activation Data**

In addition, for the Security Administrators and Certificate Authority Administrators, their user-names and password check values are stored in the Entrust/Security Manager™ database.

## **6.5 COMPUTER SECURITY CONTROLS**

The PKI hardware and software will be dedicated to performing one task: the operation of the PKI (which includes generation of digital certificates and revocations lists). There will be no other applications, hardware devices, network connections, or component software installed which are not required as part of the CA operational design. Any network ports or services that are not necessary for the operation of the PKI services will be disabled. The CA software verifies configuration via check-sum upon start-up to detect unauthorized modification to the CA software or configuration. Configuration changes are documented in audit logs. A formal configuration methodology will be used for installation and ongoing maintenance of the PKI system.

CA access control records will be maintained and audited periodically. Maintenance and service personnel will be escorted and supervised.

All updates to the Certificate Authority and Master Directory computers will first be applied and tested on test platforms before being applied to the production computers. Proper change management procedures will be followed when updating the production systems.

### **6.5.1 Specific Computer Security Technical Requirements**

The CA host computer will include the following functionality either provided by the operating system, or through a combination of operating system, CA application, and physical safeguards:

- Access control to CA services and roles;
- Access to the Entrust/Security Manager™ database and audit trails is restricted ;
- Enforced separation of duties for CA roles;
- Operating system enforces password based identification and authentication of all administrators;
- Identification and authentication of CA roles and associated identities;
- Object re-use for CA random access memory;
- Use of cryptography for session communication and database security;
- Key management plan integral to CA design;
- Archival of CA and history and audit data;
- Audit of security related events;
- Self-test of security related CA services;
- Before an update or upgrade is conducted, all software will be verified as being the valid product/version/level and is from the proper vendor.

- Trusted path for identification of CA roles and associated identities; and
- Recovery mechanisms for keys and the CA application.
- RA and LRA workstations will be physically protected via the boot-lock feature and the password protected screen saver feature.

This functionality is active and logged in the appropriate logs.

### **6.5.2 Computer Security Rating**

According to FIPS 199 definitions, the security rating of the State of Illinois PKI would be Moderate.

## **6.6 LIFE-CYCLE SECURITY CONTROLS**

The effectiveness and appropriateness of the security settings described in this CPS are reviewed as part of the audit procedures specified in the CP.

### **6.6.1 System Development Controls**

Not applicable to the State of Illinois Operational Authority (OA) as it does not develop system software for the PKI environment. All software deployed by the Illinois PKI is considered "COTS" and development methodologies associated with this environment are controlled by each vendor's controlled process or as designated by an acceptable designation, i.e. Common Criteria, FIPS 140, NIAP, or CMM models; this list is not all inclusive.

### **6.6.2 Security Management Controls**

Any new software received will first be installed and tested on an existing test environment before being put into production. The process of putting a new version of software or application into production will follow approved State change management procedures.

### **6.6.3 Life Cycle Security Ratings**

Not applicable: Dependent on vendor standards.

## **6.7 NETWORK SECURITY CONTROLS**

Remote access to Entrust/Authority™ via the Entrust/RA interface is secured using the security features of the PKIX protocol and Entrust/Session Features such as inbound FTP are disabled.

The network connection to the Entrust/Authority server and repository is protected by a firewall. The firewall will be configured with a "deny everything except that which is expressly permitted" security stance. Only the specific addresses, protocols, and ports that are needed will be permitted at each layer.



#### **6.7.1 Cryptographic module protection**

All hardware cryptographic modules associated with the Root CA will be removed and stored in a secure location when not in use. The State of Illinois Root CA will use only tokens and token readers that have been certified by the National Institute of Standards and Technology program standard for cryptography as FIPS 140-1 level 3 certified.

#### **6.7.2 Cryptographic Module Engineering Controls**

The Entrust software cryptographic module is validated to comply with FIPS 140-1 level 1. The cryptographic module(s) used for CA, RA, and LRA functions may be evaluated at FIPS 140-1 level 3 using optional cryptographic hardware modules.

### **6.8 *TIME STAMPING***

Ntpdate contacts an internal server, at 10 minutes after every hour, corrects the time and then terminates. Ntpdate is executed as a scheduled cron job within AIX.

## 7. CERTIFICATE, CARL/CRL, AND OCSP PROFILES FORMAT

### 7.1 CERTIFICATE PROFILE

The State CA issues X.509 Version 3 Certificates and supports the following fields:

- Version: Version field is set to v3.
- Serial number: When a new Subscriber Certificate is created, a unique serial number within the CA security domain is generated by Entrust/Authority. (This should not be confused with the serial number generated by the RA which is used to make the distinguished name unique.)
- Signature: Identifier for the algorithm used by the CA to sign the Certificate.
- Issuer: Certificate issuer (CA) Distinguished Name.
- Validity: Certificate validity period – not before start date and not after end date are specified.
- Subject: Certificate subject Distinguished Name.
- Subject public key information: Algorithm identifier (RSA with SHA-1), and public key.
- Extensions: See section 7.1.2 below.

#### 7.1.1 Version Numbers

Certificates issued by this CA are issued with the version number set to v3.

#### 7.1.2 Certificate Extensions

A number of X.509 version 3 Certificate extensions are included in Certificates issued by this CA. These are outlined in section 7.1.2.1 below. The X.509 version 3 Certificate extensions which are never present in Certificates issued by this CA are outlined in section 7.1.2.2 below.

##### 7.1.2.1 Supported extensions

The following fields of the X.509 version 3 Certificate format are used in this PKI:

X.509 v3 Certificate Extension	Critical/ Non Critical	Optional	Notes
SubjectAltName	Non critical	Optional	GeneralName – choices [0], [3] and [5] are not implemented.

<b>X.509 v3 Certificate Extension</b>	<b>Critical/ Non Critical</b>	<b>Optional</b>	<b>Notes</b>
AuthorityKeyIdentifier	Non critical	Not optional	only element [0] (authorityKeyIdentifier) is filled in  contains a 20 byte hash of the subjectPublicKeyInfo in the CA Certificate
SubjectKeyIdentifier	Non critical	Not optional	contains a 20 byte hash of the subjectPublicKeyInfo in the Certificate
BasicConstraints	Non critical	Not optional	only the cA Boolean is used
CRLDistributionPoints	Non critical	Not optional	if interworking with earlier Entrust releases is required - set to non critical, otherwise set to critical  Both the distribution point distinguished name and the complete URL address is included in the extension. The URL is used by relying parties outside of the State of Illinois environment.
KeyUsage	critical	Not optional	
CertificatePolicies	Non critical	Not optional	only policyIdentifier element is supported with up to 10 OIDs  policyQualifiers not supported

#### **7.1.2.2 *Unsupported extensions***

The following X.509 version 3 Certificate extensions are not used in this PKI:

- name constraints
- policy constraints
- issuer alternative name
- subject Directory attributes

#### **7.1.2.3 *Private Extensions***

The proprietary Netscape extension “NetscapeCertType” is present in the CA root certificate.

#### 7.1.2.4 State of Illinois CA Certificate Profile

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>Base certificate fields</b>				
<b>version</b>	M	N/A	2	Indicates version 3 certificate
<b>serialNumber</b>	M	N/A	A positive integer Old CA: 3a 66 02 7b New CA: will be updated.	This value will change after the CA key update.
<b>Signature</b>	M	N/A	<b>algorithm</b> is populated with the OID of the PKCS #1 SHA-1 With RSA algorithm <b>parameters</b> may be present depending on the algorithm	
<b>issuer</b>	M	N/A	OU=CMS CA OU=CMS O=State of Illinois C=US	
<b>Validity</b>	M	N/A	<b>notBefore</b> and <b>notAfter</b> are both included in <b>UTCtime</b> format YYMMDDHHMMSSZ  Old CA <b>notBefore:</b> 1/17/2001 15:07:19 PM <b>notAfter:</b> 1/17/2021 15:37:19 PM  New CA <b>notBefore:</b> will be updated <b>notAfter:</b> will be updated	This value will change after the CA key update.
<b>subject</b>	M	N/A	OU=CMS CA OU=CMS O=State of Illinois C=US	
<b>subjectPublicKeyInfo</b>	M	N/A	<b>algorithm</b> is populated with the OID of the approved algorithm (PKCS #1 RSA Encryption) <b>subjectPublicKey</b> is present	The <b>subjectPublicKey</b> will be updated after the CA key update

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>Extensions</b>				
<b>netscapeCertificateType</b>	M	nc	SSL Certificate Authority Email Certificate Authority Object Signer	
<b>cRLDistributionPoints</b>	O	nc	X.500 Name: CN = CRL1 OU = CMS CA OU = CMS O = State of Illinois C = US	
<b>keyUsage</b>	M	c	<b>keyCertSign</b> and <b>cRLSign</b> bits are set.	The criticality has been changed from non-critical to critical.
<b>authorityKeyIdentifier</b>	M	nc	<b>keyIdentifier</b> is present SM V7 CA includes hash of the public key used to verify the CA signature on the certificate <b>authorityCertIssuer</b> and <b>authorityCertSerialNumber</b> are excluded	
<b>subjectKeyIdentifier</b>	M	nc	SM V7 CA includes hash of the <b>subjectPublicKey</b> component of the <b>subjectPublicKeyInfo</b> field of the certificate	The extension will be updated after the CA key update
<b>basicConstraints</b>	M	nc	<b>ca</b> boolean is set to TRUE <b>pathLenConstraint</b> is excluded	
<b>entrustVersInfo</b>	M	nc	Current value: Entrust Authority Security Manager Version=V5.0:4.0 Key Update Allowed=Yes Certificate Category=Enterprise	A new SM V7 value will appear in this certificate after the CA key update.

FIELD/EXTENSION	P	C	VALUE	COMMENTS
			This will be updated with the V7 information during the CA key update.	
<b>certificatePolicies</b>	O	nc	This extension is currently not used but the following CP OIDs will be added: 2.16.840.114273.1.1.1.1 2.16.840.114273.1.1.1.2 2.16.840.114273.1.1.1.3 2.16.840.114273.1.1.1.4 2.16.840.114273.1.1.1.5 2.16.840.114273.1.1.1.6 2.16.840.114273.1.1.1.7 2.16.840.114273.1.1.2.1	The 8 CP OIDs will appear on the CA certificate after the CA key update.
<b>privateKeyUsagePeriod</b>	O	nc	<b>notBefore</b> and <b>notAfter</b> are present	

#### 7.1.2.5 State of Illinois Link Certificate

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>Base certificate fields</b>				
<b>version</b>	M	N/A	2	Indicates version 3 certificate
<b>serialNumber</b>	M	N/A	a positive integer	Unique value for each certificate issued by the CA
<b>signature</b>	M	N/A	<b>algorithm</b> is populated with the OID of the PKCS #1 SHA-1 With RSA algorithm  <b>parameters</b> may be present depending on the algorithm	
<b>issuer</b>	M	N/A	OU=CMS CA	Value of <b>issuer</b> and

FIELD/EXTENSION	P	C	VALUE	COMMENTS
			OU=CMS O=State of Illinois C=US	subject fields are identical
validity	M	N/A	notBefore and notAfter are both included in UTCTime format YYMMDDHHMMSSZ	
subject	M	N/A	OU=CMS CA OU=CMS O=State of Illinois C=US	Value of issuer and subject fields are identical
subjectPublicKeyInfo	M	N/A	algorithm is populated with the OID of the approved algorithm (PKCS #1 RSA Encryption) subjectPublicKey is present	
<b>Extensions</b>				
netscapeCertificateType	M	nc	SSL Certificate Authority Email Certificate Authority Object Signer	
authorityKeyIdentifier	M	nc	keyIdentifier is present SM V7 CA includes hash of the public key used to verify the CA signature on the certificate authorityCertIssuer and authorityCertSerialNumber are excluded	
subjectKeyIdentifier	M	nc	SM V7 CA includes hash of the subjectPublicKey component of the subjectPublicKeyInfo field of the certificate	
basicConstraints	M	c	cA boolean is set to TRUE pathLenConstraint is excluded	
keyUsage	M	c	keyCertSign and crlSign bits are set.	This should be set to critical (FBCA requirement)

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>entrustVersInfo</b>	M	nc	Entrust Authority Security Manager Version=V7.0  Key Update Allowed=Yes  Certificate Category=[to be determined]	
<b>cRLDistributionPoints</b>	M	nc	<p><b>distributionPoint</b> is present</p> <ul style="list-style-type: none"> <li><b>directoryName</b> is present</li> <li><b>uniformResourceIdentifier</b> is present</li> </ul> <p><b>reasons</b> and <b>cRLIssuer</b> are excluded</p> <p>[1]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>Directory Address:</p> <p>CN=CRL1</p> <p>OU=CMS CA</p> <p>OU=CMS</p> <p>O=State of Illinois</p> <p>C=US</p> <p>[2]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=ldap://servers.cmc.state.il.us/ ou=CMS%20CA,ou=CMS,o=State%20of%20Illinois, c=US?certificateRevocationList</p>	Modification to the 2 <sup>nd</sup> CDP to point to the Sol load-balanced SDSAs (ldap://servers.cmc.state.il.us/).
<b>certificatePolicies</b>	M	c	<b>policyIdentifier</b> includes State of Illinois CP OIDs for all certificate	



FIELD/EXTENSION	P	C	VALUE	COMMENTS
			types and all assurance levels that the CA is permitted to issue  <code>policyQualifiers</code> is excluded	
<code>extKeyUsage</code>	O	nc	<code>KeyPurposeID</code> contains OID 1.2.840.113533.7.7.74.3	Included only in link certificates that contain a new CA public key signed with an old CA private key. This signals to clients that their root of trust can be updated to the new CA key.
<code>authorityInfoAccess</code>	O	nc	CA certificate LDAP and HTTP URIs <ul style="list-style-type: none"> <li>LDAP URI: ldap://servers.cmc.state.il.us/ou=CMS%20CA,ou=CMS,o=State%20of%20Illinois,c=US?cACertificate;binary</li> <li>HTTP URI: http://www.illinois.gov/pki/docs/State%20of%20Illinois%20Root.p7c</li> </ul>	Should include the CA AIA (FBCA requirement)

#### 7.1.2.6 State of Illinois Subscriber Certificate

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>Base certificate fields</b>				
<code>version</code>	M	N/A	2	Indicates version 3 certificate
<code>serialNumber</code>	M	N/A	a positive integer	Unique value for each certificate issued by the CA
<code>signature</code>	M	N/A	<code>algorithm</code> is populated with the OID of the PKCS #1 SHA-1 With RSA algorithm  <code>parameters</code> may be present depending on the algorithm	
<code>issuer</code>	M	N/A	OU = CMS CA	

FIELD/EXTENSION	P	C	VALUE	COMMENTS
			OU = CMS  O = State of Illinois  C = US	
<b>validity</b>	M	N/A	<b>notBefore</b> and <b>notAfter</b> are both included in the <b>utcTime</b> format YYMMDDHHMMSSZ	
<b>subject</b>	M	N/A	Complete Distinguished Name (DN) of subject EE, encoded in <b>PrintableString</b>  Example: CN = Mark Anderson, OU = CMS CA  OU = CMS, O = State of Illinois, C = US	
<b>subjectPublicKeyInfo</b>	M	N/A	<b>algorithm</b> is populated with the OID of the approved algorithm (PKCS #1 RSA Encryption)  <b>subjectPublicKey</b> is present	
<b>Extensions</b>				
<b>certificatePolicies</b>	M	nc	<b>policyIdentifier</b> includes one OID associated with the State of Illinois assurance level.	The CP OID (2.16.840.114273.1.1) will be removed from the end-entity certificate.
<b>entrustExportInfo</b>	M	nc		
<b>subjectAltName</b>	O	nc	<b>rfc822Name</b> is included Example:  RFC822 Name=mark_anderson@cms.state.il.us  RFC822 Name=mark.anderson@illinois.gov	
<b>subjectDirectoryAttributes</b>	O	nc	For users in an administrative role (e.g. Administrators, Security Officers etc), the <b>entrustUserRole</b> attribute (OID – 1.2.840.113533.7.68.29) is included with a single INTEGER value indicating the user's role. For Administrators the INTEGER has value 1. For Security Officers the INTEGER has value 0.  Other attributes may also be optionally	

FIELD/EXTENSION	P	C	VALUE	COMMENTS
			included	
<b>cRLDistributionPoints</b>	M	nc	<p><b>distributionPoint</b> is present</p> <ul style="list-style-type: none"> <li><b>directoryName</b> is present</li> <li><b>uniformResourceIdentifier</b> is present</li> </ul> <p><b>reasons</b> and <b>cRLIssuer</b> are excluded</p> <p>[1]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>Directory Address:</p> <p>CN=CRLxxxxx</p> <p>OU=CMS CA</p> <p>OU=CMS</p> <p>O=State of Illinois</p> <p>C=US</p> <p>[2]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=ldap://servers.cmcf.state.il.us/ ou=CMS%20CA,ou=CMS,o=State%20of%20Illinois, c=US?certificateRevocationList</p>	Modification to the 2 <sup>nd</sup> CDP to point to the Sol load-balanced SDSA (ldap://servers.cmcf.state.il.us/).
<b>keyUsage</b>	M	c	<p><b>digitalSignature</b> bit is set for verification certificates</p> <p><b>nonRepudiation</b> bit is set for verification certificates</p> <p><b>keyEncipherment</b> bit is set for encryption certificates</p>	
<b>authorityKeyIdentifier</b>	M	nc	<p><b>keyIdentifier</b> is present</p> <p>SM V7 CA includes hash of the public key used to verify the CA signature on the</p>	

FIELD/EXTENSION	P	C	VALUE	COMMENTS
			certificate	
<b>subjectKeyIdentifier</b>	M	nc	SM V7 CA includes hash of the <b>subjectPublicKey</b> component of the <b>subjectPublicKeyInfo</b> field of the certificate	
<b>basicConstraints</b>	M	nc	<b>cA</b> boolean set to <b>FALSE</b> <b>pathLenConstraint</b> is excluded	
<b>entrustVersInfo</b>	M	nc	Entrust Authority Security Manager Version=V7.0  Key Update Allowed=Yes  Certificate Category=Enterprise	
<b>privateKeyUsagePeriod</b>	O	nc		Included in verification certificates  Excluded from encryption certificates
<b>authorityInfoAccess</b>	N/A	nc	CA certificate LDAP and HTTP URIs  <ul style="list-style-type: none"> <li>LDAP URI: ldap://server.cmc.state.il.us/ou=CMS%20CA,ou=CMS,o=State%20of%20Illinois,c=US?cACertificate;binary]</li> <li>HTTP URI: http://www.illinois.gov/pki/docs/State%20of%20Illinois%20Root.p7c</li> </ul>	

#### 7.1.2.7 State of Illinois Cross-certificate

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>Base certificate fields</b>				
<b>version</b>	M	N/A	2	Indicates version 3 certificate

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>serialNumber</b>	M	N/A	a positive integer	Unique value for each certificate issued by the CA
<b>signature</b>	M	N/A	<b>algorithm</b> is populated with the OID of the PKCS #1 SHA-1 With RSA algorithm  <b>parameters</b> may be present depending on the algorithm	
<b>issuer</b>	M	N/A	OU=CMS CA OU=CMS O=State of Illinois C=US	
<b>validity</b>	M	N/A	<b>notBefore</b> and <b>notAfter</b> are both included in <b>UTCTime</b> format YYMMDDHHMMSSZ	
<b>subject</b>	M	N/A	OU = Entrust  OU = FBCA  O = U.S. Government  C = US	
<b>subjectPublicKeyInfo</b>	M	N/A	<b>algorithm</b> is populated with the OID of the approved algorithm (PKCS #1 RSA Encryption)  <b>subjectPublicKey</b> is present	
<b>Extensions</b>				

FIELD/EXTENSION	P	C	VALUE	COMMENTS
<b>policyMappings</b>	O	nc	<p><b>issuerDomainPolicy</b> includes a State of Illinois CP OID</p> <p><b>subjectDomainPolicy</b> includes an OID representing an equivalent policy in another domain (e.g. FBCA)</p> <p>[1]Issuer Domain=2.16.840.114273.1.1.1.1</p> <p>Subject Domain=2.16.840.1.101.3.2.1.3.2</p> <p>[2]Issuer Domain=2.16.840.114273.1.1.1.2</p> <p>Subject Domain=2.16.840.1.101.3.2.1.3.2</p> <p>[3]Issuer Domain=2.16.840.114273.1.1.1.3</p> <p>Subject Domain=2.16.840.1.101.3.2.1.3.3</p> <p>[4]Issuer Domain=2.16.840.114273.1.1.1.4</p> <p>Subject Domain=2.16.840.1.101.3.2.1.3.12</p> <p>[5]Issuer Domain=2.16.840.114273.1.1.1.5</p> <p>Subject Domain=2.16.840.1.101.3.2.1.3.3</p> <p>[6]Issuer Domain=2.16.840.114273.1.1.1.6</p> <p>Subject Domain=2.16.840.1.101.3.2.1.3.12</p> <p>7]Issuer Domain=2.16.840.114273.1.1.1.7</p> <p>Subject Domain=2.16.840.1.101.3.2.1.3.12</p>	This extension needs to be modified to include 4 policy mappings.
<b>subjectKeyIdentifier</b>	M	nc	SM V7 CA populates with value provided by subject CA in certificate request. If no value supplied, SM V7 CA will calculate value as hash of the <b>subjectPublicKey</b> component of the <b>subjectPublicKeyInfo</b> field of the certificate	
<b>cRLDistributionPoints</b>	M	nc	<p><b>distributionPoint</b> is present</p> <ul style="list-style-type: none"> <li><b>directoryName</b> is present</li> <li><b>uniformResourceIdentifier</b> is present</li> </ul> <p><b>reasons</b> and <b>cRLIssuer</b> are excluded</p>	Modification to the 2 <sup>nd</sup> CDP to point to the Sol load-balanced SDSA (ldap://servers.cmc.state.il.u

FIELD/EXTENSION	P	C	VALUE	COMMENTS
			<p>[1]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>Directory Address:</p> <p>CN=CRL1</p> <p>OU=CMS CA</p> <p>OU=CMS</p> <p>O=State of Illinois</p> <p>C=US</p> <p>[2]CRL Distribution Point</p> <p>Distribution Point Name:</p> <p>Full Name:</p> <p>URL=ldap://servers.cmc.state.il.us/ ou=CMS%20CA,ou=CMS,o=State%20of%20Illinois, c=US?certificateRevocationList</p>	s/).
<b>keyUsage</b>	M	c	<b>keyCertSign</b> and <b>cr1Sign</b> bits are set.	
<b>authorityKeyIdentifier</b>	M	nc	<p><b>keyIdentifier</b> is present</p> <p>SM V7 CA includes hash of the public key used to verify the CA signature on the certificate</p> <p><b>authorityCertIssuer</b> and <b>authorityCertSerialNumber</b> are excluded</p>	
<b>entrustVersInfo</b>	M	nc	<p>Entrust Authority Security Manager Version=V7.0</p> <p>Key Update Allowed=Yes</p> <p>Certificate Category=XCert</p>	
<b>basicConstraints</b>	M	c	<p><b>cA</b> boolean set to <b>TRUE</b></p> <p><b>pathLenConstraint</b> not included</p>	
<b>authorityInfoAccess</b>	O	nc	<p>CA certificate LDAP and HTTP URIs</p> <ul style="list-style-type: none"> <li>LDAP URI:</li> </ul>	

FIELD/EXTENSION	P	C	VALUE	COMMENTS
			ldap://servers.cmc.state.il.us/ou=CMS%20CA,ou=CMS,o=State%20of%20Illinois,c=US?cACertificate;binary]  • HTTP URI: <a href="http://www.illinois.gov/pki/docs/State%20of%20Illinois%20Root.p7c">http://www.illinois.gov/pki/docs/State%20of%20Illinois%20Root.p7c</a>	
certificatePolicies	O	nc	The following CP OIDs will be added in this extension: 2.16.840.114273.1.1.1.1  2.16.840.114273.1.1.1.2  2.16.840.114273.1.1.1.3  2.16.840.114273.1.1.1.4  2.16.840.114273.1.1.1.5  2.16.840.114273.1.1.1.6  2.16.840.114273.1.1.1.7	

### 7.1.3 Algorithm Object Identifiers

The State CA supports the following algorithms for signing or transmission of data:

#### Asymmetric - Key Exchange

- RSA in accordance with PKCS#1.
- Diffie-Hellman.

#### Asymmetric - Digital Signature

- DSA in accordance with DSS (FIPS PUB 186 and ANSI X9.30 (Part 1)).
- RSA in accordance with PKCS#1.
- Hash Functions
- MD5 in accordance with RFC 1321.
- SHA-1 in accordance with FIPS PUB 180-1 and ANSI X9.30 (Part 2).
- Symmetric - Bulk Encryption



- CAST- (CBC mode) in accordance with FIPS PUB 81, ANSI X3.106 and ISO/IEC 10116 (RFC 2144).
- DES in accordance with FIPS PUB 46-2 and ANSI X3.92.
- Triple DES (CBC mode) in accordance with FIPS PUB 81, ANSI X3.106 and ISO/IEC 10116.
- RC2 (40-128bit CBC mode) in accordance with FIPS PUB 81, ANSI X3.106 and ISO/IEC 10116.

#### **7.1.4 Name Forms**

In a Certificate, the issuer DN and subject DN fields contain the full X.500 Distinguished Name of the Certificate issuer or Certificate subject. If the subjectAltName extension is present in a Certificate, it contains the Certificate subject's rfc822Name (email address).

#### **7.1.5 Name Constraints**

Name constraints are not used in this PKI.

#### **7.1.6 Certificate Policy Object Identifier**

Multiple Certificate Policies are supported by the Illinois PKI and are applicable to the operation and issuance of certificates supported by the Root CA, and are identified in section 1.2 of this CPS.

#### **7.1.7 Usage of Policy Constraints Extension**

Policy constraints are not used in the Illinois PKI certificate profile.

#### **7.1.8 Policy Qualifiers Syntax & Semantics**

Policy qualifiers are not used in the Illinois PKI certificate profile.

#### **7.1.9 Processing Semantics for the Critical Certificate Policy Extension**

The only critical certificate extensions issued by the Illinois Root CA are the cRLDistributionPoints extension and the KeyUsage extension. The CRL or ARL will always be retrieved by either using the directory entry indicated in the certificate, or by using the URL indicated in the certificate, unless a current copy of that CRL or ARL is cached by Entrust/Entelligence software client.

### **7.2 CRL PROFILE**

The following fields of the X.509 version 2 CRL format are used in this PKI:

- version: set to v2
- signature: identifier of the algorithm used to sign the CRL

- issuer: the full Distinguished Name of the CA issuing the CRL
- Effective date: time of CRL issue
- next update: time of next expected CRL update
- revoked Certificates: list of revoked Certificate information

### 7.2.1 Version Numbers

CRLs issued by this CA are X.509 version 2 CRLs.

### 7.2.2 CRL Entry Extensions

The X.509 version 2 CRL extensions used in this PKI are outlined in section 7.2.2.1 below.

#### 7.2.2.1 Supported Extensions

The following CRL and CRL entry extensions are used in this PKI:

X.509 v2 CRL Extension	Critical/ Non Critical	Optional	Notes
AuthorityKeyIdentifier	Non critical	Not optional	only element [0] (authorityKeyIdentifier) is filled in  contains a 20 byte hash of the subjectPublicKeyInfo in the CA Certificate
CRLNumber	Non critical	Not optional	Incremented each time a particular CRL/ARL is changed
IssuingDistribution Point	Critical	Not optional	element [0] (distributionPoint) includes the full DN of the distribution point  element [1] (onlyContainsUserCerts) is included for CRLs  element [2] (onlyContainsCACerts) is included for ARLs  element [1] and [2] are never present together in the same revocation list  elements [3] and [4] are not used

### **7.3 OCSP PROFILE**

Not supported.

## **8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS**

In order to ensure compliance with policies and practices, an annual compliance audit will be conducted of the State of Illinois PKI in accordance with Certificate Policy section 8.

### **8.1 FREQUENCY OF AUDIT OR ASSESSMENTS**

The CA will undergo a compliance audit prior to initial approval as a CA to demonstrate compliance with State Policies and the CP and CPS. Subsequent compliance audits will be required every twelve months, or whenever substantive changes are made to the CP or the CPS.

The auditing of the Root Key Generation Ceremony is considered the initial audit for the purposes of this Certificate Policy.

Subsequent audits will be conducted either by an independent auditor contracted by the Department of Central Management Services, or in conjunction with the annual IT compliance audit of the Department of Central Management Services Bureau of Communication & Computer Services.

### **8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR**

The State of Illinois PKI will utilize the following criteria when choosing an auditor to perform the PKI compliance audit:

Annual audits will be performed by independent auditors selected by the State of Illinois. Auditors must demonstrate competence in the field of compliance audits and must regularly perform such compliance audits as a primary responsibility.

### **8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY**

Annual audits will be performed either by third party independent auditors contracted specifically for the purpose of auditing the State's PKI operations, or by auditors employed by the State of Illinois who are independent of the OA or PA.

### **8.4 TOPICS COVERED BY ASSESSMENT**

The annual audit will investigate the operations of the CA and RA functions of the State PKI to ensure their compliance with the CP and the CPS. Some areas of focus for these audits will be (but are not limited to):

- **Identification & Authentication**  
Initial Registration

Routine Rekey

Rekey after Revocation

Revocation Request

- **Operational Requirements**

- Certificate Application

- Certificate Issuance

- Certificate Acceptance

- Key Recovery

- Certificate Suspension/Revocation

- Computer Security Audit Procedures

- Records Archival

- CA key Changeover

- Compromise and Disaster Recovery

- CA Termination

- **Physical, Procedural & Personnel Security**

- Physical Security Controls

- Procedural Controls

- Personnel Security Controls

- **Technical Security Controls**

- Key Pair Generation & Installation

- Private Key Protection

- Other Aspects of Key Pair Management

- Activation Data

- Computer Security Controls

- Lifecycle Security Controls

Network Security Controls

Cryptographic Module Engineering Controls

- **Certificate & CRL Profiles**

Certificate Profile

CRL Profile

- **Specification Administration**

Contact Information

Specification Change Procedures

Publication and Notification Procedures

Approval Procedures

## **8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY**

If a deficiency is identified by the auditor, the State PA will, based upon the findings of the auditor, determine which of the following actions will be taken in accordance with Certificate Policy section 8.5:

- a.) Continue to operate as usual;
- b.) Continue to operate but with limitations on rights; or
- c.) Suspend operation

If action a) or b) is taken the State PA and OA will be responsible for ensuring that corrective actions are taken within a reasonable period. At that time, or earlier if agreed by the PA and auditor, the audit team will reassess. If, upon reassessment, corrective actions have not been taken, the PA will determine if more severe action (e.g. action c) above) is required.

If action c) is taken all certificates issued by the CA, including end-user certificates will be revoked prior to suspension of the service. The State PA and OA are responsible for reporting the status of corrective action to the auditors on a weekly basis. The PA and auditor together will determine when the re-assessment is to occur. Upon reassessment, if the deficiencies have been corrected, the CA will resume service and new certificates will be issued to Certificate users.

## **8.6 COMMUNICATION OF RESULTS**

Results of the annual audit will be provided to the State PA, The State of Illinois Department of Central Management Services' Chief Security Officer, and the Auditor General. The State PA, with input from the auditor, will determine if Certificate users need to be informed of any action as a result of the audit. The State PA will communicate to Certificate users via the internet at <http://www.illinois.gov/pki> .

## **9. OTHER BUSINESS AND LEGAL MATTERS**

### **9.1 FEES**

No direct fees will be assessed by the CA or OA.

In cross-certification or hosting agreements with business partner organizations, the costs will be expected to balance naturally between the State and the business partner organization. Any exceptions, which may result in additional fees for any of the services outlined in this section and its subsections, will be addressed in the specific cross-certification agreement itself.

#### **9.1.1 Certificate Issuance/Renewal Fees**

The Illinois PKI will issue, renew, and revoke Subscribers certificates at no cost.

#### **9.1.2 Certificate Access Fees**

The Illinois PKI will not impose any certificate access fees on Subscribers with respect to its own Certificate(s) or the status of such Certificate(s).

#### **9.1.3 Revocation or Status Information Access Fee**

The State will not impose fees for certificate revocation or status services.

#### **9.1.4 Fees for other Services**

The Illinois PKI will not impose fees for access to policy information.

#### **9.1.5 Refund Policy**

Because no fees will be charged for certificate services, as specified in this CPS or by the Illinois PKI, there is no need to provide procedures for refunds.

### **9.2 FINANCIAL RESPONSIBILITY**

No stipulation.

Interested parties will refer to section 9.2 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

#### **9.2.1 Insurance Coverage**

No stipulation.



### **9.2.2 Other Assets**

No stipulation.

### **9.2.3 Insurance/warranty Coverage for End-Entities**

No stipulation.

## **9.3 CONFIDENTIALITY OF BUSINESS INFORMATION**

The State of Illinois PKI will maintain the confidentiality of certain information in accordance with Certificate Policy section 9.3 and its sub-sections. In accordance with Certificate Policy section 9.3, the CA, RA, or any LRA will not disclose certificate or certificate-related information to any third party except when:

- authorized to do so by the CP,
- required to be disclosed by law or court order, or
- authorized to do so by the certificate holder

Any requests for disclosure of information must be signed and submitted to the CA. The CA will communicate all such requests to the PA.

All subscriber information is considered confidential and is kept under lock and key. Only members of the Operational Authority have access to the subscriber information.

### **9.3.1 Scope of Confidential Information**

In accordance with Certificate Policy section 9.3, the following provisions will apply:

The Subscriber's private signing key must be kept confidential by the Subscriber. The CA and RA are not provided any access to those keys. The Subscriber's private encryption key must be kept confidential by the Subscriber; however, the CA may recover private encryption keys for State of Illinois employees as described in Section 4.7 (Key Recovery) of the CP. Personal information held by the CA, other than that which is explicitly published as part of a certificate, CRL, certificate policy, or this document is considered confidential and will not be released unless required by law.

In addition, personal information submitted to the CA by Subscribers:

- Must be made available to the subscriber for individual review following an authenticated request by said subscriber;
- Must be subject to correction and/or update by said subscriber; and

- Must be protected by the CA in such a way as to ensure the integrity of said collected personal identifiable information.

### **9.3.2 Information not within the scope of Confidential Information**

Information included in public certificates and CRLs issued by the CA are not considered confidential. Likewise, information contained in the public repository is not considered confidential.

### **9.3.3 Responsibility to Protect Confidential Information**

When a certificate is revoked by the CA, a revocation reason code will be included in the CRL entry for the revoked certificate. This revocation reason code is not considered confidential and can be shared with all users and Relying Parties. No other details concerning the revocation of a certificate will be disclosed by the Illinois PKI.

## **9.4 *PRIVACY OF PERSONAL INFORMATION***

### **9.4.1 Privacy Plan**

No stipulation.

### **9.4.2 Information treated as Private**

All subscriber information should be treated as private information. As such, it should be stored in a locked cabinet in a room which can be locked when staff is not present.

### **9.4.3 Information not deemed Private**

No stipulation.

### **9.4.4 Responsibility to Protect Private Information**

Sensitive information will be stored securely, and may be released only in accordance with other stipulations in Section 9.4.7 of the Certificate Policy.

### **9.4.5 Notice and Consent to use Private Information**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

### **9.4.6 Disclosure Pursuant to Judicial/Administrative Process**

- The PA and OA will comply with all official, authorized, and verifiable court orders to recover a Subscriber's keys.

- Prior to recovering the Subscriber's profile, the CA will alter the Distinguished Name by appending the word "Recovered", then the Subscriber's Certificate will be recovered and the profile will be delivered to the Agency LRA on physical media. The LRA will sign for receipt of the profile, will supervise all Agency use of the recovered key for the purposes described in the approved request and will certify that the profile was destroyed when those uses are completed. Then, the Subscriber's Certificate will be revoked following the procedures in Section 4.9 "Certificate Revocation".
- A Subscriber whose profile has been revoked as part of an involuntary recovery must follow the procedures described in Section 3.3 to be re-authenticated and issued a new Certificate.

#### **9.4.7 Other Information Disclosure Circumstances**

If a subpoena seeking information that is considered confidential under the Certificate Policy is provided to the Operational Authority, the Operational Authority shall consult with legal counsel and will follow whatever directives are given by said counsel.

No Stipulation for owner request for disclosure.

### **9.5 *INTELLECTUAL PROPERTY RIGHTS***

No stipulation.

### **9.6 *REPRESENTATIONS & WARRANTIES***

#### **9.6.1 CA Representations and Warranties**

The OA's responsibility is to "Provide CA services with a maximum available application target of 100% and allowing for normal maintenance" (CP section 9.6.1). To accomplish this task, the following steps will be taken:

- Both the CA and Directory computers will be designated as "High Availability" boxes with IBM's HACMP software providing the failover capabilities. A "heartbeat" signal will be utilized to indicate that failover is necessary.
- Multiple servers will run the Entrust Profile server software to allow roaming logins. These servers will be load balanced w/failover using the Content Switching Modules (CSM) on the mainframe.

- Multiple servers will run the DIRX shadow directories to allow access to repository information. These servers will be load balanced w/failover using the Content Switching Modules (CSM) on the mainframe.

### **9.6.2 RA Representations and Warranties**

The RA or LRA will verify the accuracy and authenticity of the information provided by Subscribers to the RA or LRA at the time of application for a certificate. Pursuant to the terms of a valid Subscriber Agreement, the RA or LRA may make use of the State employment records to verify the data by comparing the application information with information in the State databases. The RA will provide this verification on behalf of the CA.

Each LRA will verify the accuracy and authenticity of the information provided by the Subscribers to the LRA at the time of application for a certificate. The CA may, but is not required to, verify the accuracy and authenticity of information provided by Subscribers through an LRA.

#### **9.6.2.1 *Disclaimers***

No stipulation.

#### **9.6.2.2 *Loss Limitations***

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.8 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP

#### **9.6.2.3 *Other Exclusions***

No stipulation.

#### **9.6.2.4 *Hazardous Activities***

No stipulation.

### **9.6.3 Subscriber Representations and Warranties**

Subscribers are required to:

- Make true representation at all times to the CA, the RA and the appropriate LRAs regarding information in their certificates; and other identification and authentication information;
- Use certificates in a manner consistent with this Certificate Policy;
- Take reasonable precautions to prevent any compromise, modification, loss, disclosure, or unauthorized use of their private keys;

- Protect their Certificate user password;
- Upon issuance of a Certificate naming the applicant as the Subscriber, review the Certificate to ensure that all Subscriber information included in it is accurate, and to expressly indicate acceptance or rejection of the Certificate;
- Inform the RA or appropriate LRA within 48 hours of a change to any information included in their certificate or certificate application request;
- Inform the RA or appropriate LRA within 8 hours of a suspected compromise of one/both of their private keys; and
- Rightfully hold private keys corresponding to the public keys listed in their certificate.

#### **9.6.4 Relying Parties Representations and Warranties**

Relying parties will rely on a valid Certificate for purposes of verifying the digital signature only if prior to reliance, the Relying Party will:

- (1) Agree to be bound by the terms of this CP;
- (2) Verify the digital signature by reference to the public key in the Certificate;  
and
- (3) Refer to the most recent CRL.

Relying party understands that certificates are subject to revocation and such action shall not be reflected in the Certificate itself, but must be verified by consulting the most recent certificate revocation list.

#### **9.6.5 Representations and Warranties of other Participants**

None.

### **9.7 *DISCLAIMERS OF WARRANTIES***

No stipulation.

### **9.8 *LIMITATIONS OF LIABILITY***

#### **9.8.1 CA liability**

Interested parties will refer to section 9.6.1 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.4.2 of the CP.

#### **9.8.2 RA liability**

Interested parties will refer to section 9.6.1 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

### **9.9 *INDEMNITIES***

Interested parties will refer to section 9.9 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

### **9.9.1 Hold Harmless: Relying Parties**

Relying parties shall hold the State harmless from and against any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to (i) any use or reliance by a relying party on the Certificate or any service or transaction provided by the State or performed by a relying party in connection with the Certificates, (ii) lack of proper validation of a Certificate Authority (CA) certificate by a relying party, (iii) reliance by the relying party on an expired or revoked the Certificate, (iv) use of a Certificate other than as permitted by the State Certificate Policy, Certification Practice Statement, the subscriber agreement, any relying party agreement, and applicable law, (v) failure by a relying party to exercise reasonable judgment in the circumstances in relying on a Certificate, or (vi) any claim or allegation that the reliance by a relying party on a Certificate or the contents of a Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates the rights (including intellectual property rights) of any third party in any jurisdiction. Notwithstanding the foregoing, Relying Parties shall not be obligated to hold the State harmless in respect to any liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to any willful misconduct by the State.

### **9.9.2 Hold Harmless: Subscribers**

Subscriber will hold the State harmless from and against any and all liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to (i) any use or reliance by the subscriber on any Certificate or any service or transaction provided by the State or performed by the subscriber in connection with the Certificates, (ii) any misrepresentation made by subscriber in using or applying for a Certificate, (iii) modification made by subscriber to the contents of a Certificate, (iv) use of a Certificate other than as permitted by the State Certificate Policy, Certification Practice Statement, the subscriber agreement, any relying party agreement, and applicable law, (v) loss, disclosure, compromise or unauthorized use of the private key corresponding to the public key in subscriber's the Certificate, or (vi) any allegation that the use of a subscriber's the Certificate or the contents of a subscriber's the Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates the rights (including intellectual property rights) of any third party in any jurisdiction. Notwithstanding the foregoing, a subscriber will not be obligated to hold the State harmless in respect to any liabilities, losses, costs, expenses, damages, claims, and settlement amounts (including reasonable attorney's fees, court costs and experts fees) arising out of or relating to any willful misconduct by the State.

## **9.10 TERM & TERMINATION**

### **9.10.1 Term**

In the event of a conflict between the provisions of the CP and this CPS and a cross-certification agreement executed between the PA and the entity responsible for another CA, the terms of the cross-certification agreement will take precedence.

### **9.10.2 Termination**

In the event that the State CA ceases operation or is otherwise terminated:

- All Subscribers, sponsoring organizations, and Relying Parties must be promptly notified of the cessation;
- All CAs with which cross-certification agreements are current at the time of cessation will be informed so that cross-Certificates to the State CA may be revoked;
- All State Certificates issued by the State CA will be revoked no later than the time of cessation; and
- All current and archived State identity proofing, Certificate, validation, revocation/suspension, renewal, policy and practices, billing, and audit data will be archived according to the State data archive policy.

Notification methods could include but are not be limited to web site notification, mass email, media advertisements, etc.

### **9.10.3 Effect of Termination and Survival**

No stipulation.

## **9.11 INDIVIDUAL NOTICES & COMMUNICATIONS WITH PARTICIPANTS**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.4.5 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP

## **9.12 AMENDMENTS**

### **9.12.1 Procedure for Amendment**

Changes to items within this CPS which, in the judgment of the OA and PA, will have no/minimal impact on the users managed by this CA, may be made with no change to the CPS version number and no notification to the users.

Changes to the Certificate Policies supported by this CPS as well as changes to items within this CPS which, in the judgment the OA and PA may have significant impact on the users managed by this CA, may be made with 60 days notice to the user community and the version number of this CPS must be increased accordingly.

### **9.12.2 Notification Mechanism and Period**

The State CA will make available copies of the CP both online and in hard copy form. The dissemination of the complete and sensitive version of this CPS to requesting parties will be made at the sole discretion of the Policy Authority. A “sanitized” or truncated version of this CPS will be available for viewing at <http://www.illinois.gov/pki/cps.cfm> .

### **9.12.3 Circumstances under which OID must be changed**

No stipulation.

## **9.13 DISPUTE RESOLUTION PROVISIONS**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.13 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

By incorporating Subject names into State Certificates, the State does not determine whether the use of the Subject name infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property or other rights of any person, entity or organization. the State neither acts as an arbitrator nor provides dispute resolution between Subscribers and third party complainants in respect to disputes in relation to the registration or use of a Subject name in a State Certificate. This CPS does not bestow any procedural or substantive rights on any third party complainant in respect to the Subject name in a Certificate. The State will in no way be precluded from seeking legal or equitable relief (including injunctive relief) in respect to any dispute between a Subscriber and third party complainant or in respect to any dispute between a Subscriber and the State arising out of the Subject name in a State Certificate. The State will have the right to revoke a State Certificate upon receipt of a properly authenticated order from an arbitrator or court of competent jurisdiction



requiring the revocation of the State Certificate or State Certificates containing a Subject name in dispute. Since both the commonName and serialNumber attributes are used to create the RDNs for Certificate subjects, such disputes are expected to be rare.

## **9.14 GOVERNING LAW**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.14 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

## **9.15 COMPLIANCE WITH APPLICABLE LAW**

The Illinois OA will comply with applicable law.

## **9.16 MISCELLANEOUS PROVISIONS**

### **9.16.1 Entire agreement**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP

### **9.16.2 Assignment**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16.2 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

### **9.16.3 Severability**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16.3 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

### **9.16.4 Enforcement (Attorney Fees/Waiver of Rights)**

Affected parties will refer to section 9.16.4 of the Certificate Policy. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

#### **9.16.5 Force Majeure**

For information related to this topic, the enquiring party should refer to the Illinois certificate policy, Section 9.16.5 for more details and action sanctioned by the State of Illinois. Questions should be directed to the Point of contact listed in section 1.5.2 of the CP.

#### **9.17 OTHER PROVISIONS**

The express waiver by the State or the Policy Authority of any provision, condition, or requirement of this CPS will not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

## 10. BIBLIOGRAPHY

Many of the following documents were used in part to develop this CPS:

ABADSG	Digital Signature Guidelines,	1996-08-01.
	<a href="http://www.abanet.org/scitech/ec/isc/dsgfree.html">http://www.abanet.org/scitech/ec/isc/dsgfree.html</a> .	
CIMC	Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001.	
FIPS 140-2	Security Requirements for Cryptographic Modules May 25, 2001.	
	<a href="http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf">http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf</a>	
FIPS 186-2	Digital Signature Standard, January 27, 2000.	
	<a href="http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf">http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf</a>	
FOIACT	5 U.S.C. 552, Freedom of Information Act.	
	<a href="Http://www4.law.cornell.edu/uscode/5/552.html">Http://www4.law.cornell.edu/uscode/5/552.html</a>	
FPKI-Prof	Federal PKI X.509 Certificate and CRL Extensions Profile	
ISO9594-8	Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997.	
ITMRA	40 U.S.C. 1452, Information Technology Management Reform Act of 1996.	
	<a href="Http://www4.law.cornell.edu/uscode/40/1452.html">Http://www4.law.cornell.edu/uscode/40/1452.html</a>	
NAG69C	Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999.	
NSD42	National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990.	
	<a href="Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt">Http://snyside.sunnyside.com/cpsr/privacy/computer_security/nsd_42.txt</a> (redacted version)	
NS4005	NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997.	
NS4009	NSTISSI 4009, National Information Systems Security Glossary, January 1999.	
PKCS#12	Personal Information Exchange Syntax Standard, April 1997.	
	<a href="ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf">ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf</a>	
RFC 2510	Certificate Management Protocol, Adams and Farrell, March 1999.	
RFC 3647	Certificate Policy and Certification Practices Framework, Chokhani and	

Ford, Sabett, Merrill, and Wu, November 2003.

## **11. ACRONYMS AND ABBREVIATIONS**

AICPA	American Institute of Certified Public Accounts
AIX	Advanced Interactive Executive
ANSI	American National Standards Institute
CARL	Certificate Authority Revocation List
CBC	Cipher Block Chaining
CIMC	Certificate Issuing and Management Components
CMM	Capability Maturity Model
CMS	Central Management Services
COMSEC	Communications Security
COTS	Commercial off the Shelf
CPS	Certification Practice Statement
CRL	Certificate Revocation Lists
CSS	Certificate Status Server
DB2	Database 2
DES	Data Encryption Standard
DN	Distinguished Name
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
FAR	Federal Acquisition Regulations
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FPKI	Federal Public Key Infrastructure
FPKI-Prof	Federal PKI Profice
FPKIPA	Federal PKI Policy Authority
FPKISC	Federal PKI Steering Committee
FTP	File Transfer Protocol
GPEA	Government Paperwork Elimination Act
HACMP	High Availability Cluster Multi Processing
IBM	International Business Machines
IETF	Internet Engineering Task Force
IL	Illinois

ISO	International Organization for Standardization
ISSO	Information Systems Security Officer
IT	Information Technology
ITU	International Telecommunications Union
ITU-T	International Telecommunications Union Telecommunications
ITU-TSS	International Telecommunications Union Telecommunications Sector
LDAP	Lightweight Directory Access Protocol
LRA	Local Registration Authorities
MAC	Message Authentication Code
MD5	Message Digest 5
MOA	Memorandum of Agreement
N/A	Not Applicable
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PMA	Policy Management Authority
RA	Registration Authority
RDN	Relational Distinguished Name
RFC	Request for Comments
RSA	Rivest Shimar Adleman
S/MIME	Secure Multipurpose Internet Mail Extension

SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TSDM	Trusted Software Development Methodology
U.S	United States
U.S.C	United States Code
UPS	Uninterrupted Power Supply
URL	Used by Relying
USB	Universal Serial Bus
VM	Virtual Machine
VPN	Virtual Private Network
WWW	World Wide Web

## 12. GLOSSARY

Access	Ability to make use of any information system (IS) resource. [NS4009]
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009]
Accreditation	Defined in ISO-IEC Guide 2 as a: "procedure by which an authoritative body gives formal recognition that a body or person is competent to carry out specific tasks." The accrediting body is a recognized entity which accredits the auditor as qualified to perform its evaluation of CAs or other PKI components, applying standards derived from the Certificate Policies adopted by the Policy-adopting body. Examples of bodies who have or might perform such a role include NIST's National Voluntary Laboratory Accreditation Program (NVLAP), or the American Institute of Certified Public Accounts (AICPA) which accredits Third Party Auditing Firms to audit various entities.
Activation Data	Private data, other than keys, that are required to access cryptographic modules.
Applicant	The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32]
Assurance Level	A representation of how rigorously the Registration Authority authenticates the identity claimed by an Applicant prior to issuing a Certificate.
Archive	Long-term, physically separate storage.
Authority Revocation List (ARL)	A list of revoked Certificate Authority Certificates. An ARL is a Certificate Revocation List for Certificate Authority certificates.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Audit	An Independent review and examination of documentation, records and activities to assess the adequacy of system



	controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Audit Data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"]
Authenticate	To confirm the identity of an entity when that identity is presented.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Backup	Copy of files and programs made to facilitate recovery if necessary. [NS4009]
Binding	Process of associating two related elements of information. [NS4009]
Biometric	A physical or behavioral characteristic of a human being.
CA Facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
Certificate	<p>A Certificate issued under this Policy by a Certificate Authority and identified as such by the inclusion of the registered object identifier for this Certificate Policy in the Certificate Policies field, and at a minimum:</p> <ul style="list-style-type: none"> <li>• Identifies the Certificate Authority issuing it.</li> <li>• Names or otherwise identifies its Subscriber.</li> <li>• Contains a public key that corresponds to a private key under the control of the Authorized Subscriber.</li> <li>• Identifies its operational period.</li> <li>• Contains a Certificate serial number and is digitally signed by the Certificate Authority issuing it.</li> </ul> <p>The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.</p>
Certificate Authority (CA)	A Certificate Authority is an entity that is responsible for authorizing and causing the issuance of a Certificate. A Certificate Authority can perform the functions of a Registration Authority (RA) and can delegate or outsource this

function to separate entities.

A Certificate Authority performs two essential functions. First, it is responsible for identifying and authenticating the intended Authorized Subscriber to be named in a Certificate, and verifying that such Authorized Subscriber possesses the private key that corresponds to the public key that shall be listed in the Certificate. Second, the Certificate Authority actually creates and digitally signs the Authorized Subscriber's Certificate. The Certificate issued by the Certificate Authority then represents that CA's statement as to the identity of the person named in the Certificate and the binding of that person to a particular public-private key pair.

Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.
Certificate Management Authority (CMA)	A Certification Authority or a Registration Authority.
Certificate Manufacturing	The process of accepting a public key and identifying information from an authorized Subscriber, producing a digital certificate containing that and other pertinent information, and digitally signing the Certificate.
Certification Authority Software	Key Management and cryptographic software used to manage certificates issued to subscribers.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements. For example, a particular Certificate Policy might indicate applicability of a type of Certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.
Certificate Authority Software	The application software required to manufacture certificates by the CA
Certification Practice Statement (CPS)	A statement of the practices, which a Certificate Authority (CA) employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the Certificate Authority (CA) uses to satisfy the requirements specified in the CP that are supported by it.
Certificate-Related	Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing

Information	certificates.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created, time stamped and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the Certificate Authority (CA) may choose to split a CRL into a series of smaller CRLs. When an End Entity chooses to accept a certificate the Relying Party Agreement requires that this Relying Party check that the certificate is not listed on the most recently issued CRL.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Common Criteria	A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products.
Compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009]
Computer Security Objects Registry (CSOR)	Computer Security Objects Registry operated by the National Institute of Standards and Technology.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [NS4009]
Cross-Certificate	<p>A Certificate used to establish a trust relationship between two Certification Authorities.</p> <p>A Cross-Certificate is a Certificate issued by one Certificate Authority (CA) to another CA which contains a CA key associated with the private CA signature key used for issuing Certificates. Typically a cross-certificate is used to allow End Entities in one CA to communicate security with End Entities in another CA. A cross-certificate issued by CA#1 to CA#2 allows Entity #a, who has a Certificate issued by CA#1, to</p>

	accept a Certificate used by Entity #b, who has a Certificate issued by CA#2.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401]
Cryptoperiod	Time span during which each key setting remains in effect. [NS4009]
Data Integrity	Assurance that the data are unchanged from creation to reception.
Digital Signature	<p>The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine:</p> <p>Whether the transformation was created using the private signing key that corresponds to the signer's public verification key.</p> <p>Whether the message has been altered since the transformation was made.</p>
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the End Entity within the Certificate Authority (CA) domain.
Dual Use Certificate	A certificate that is intended for use with both digital signature and data encryption services.
Duration	A field within a certificate which is composed of two subfields; "date of issue" and "date of next issue".
E-commerce	The use of network technology (especially the internet) to buy or sell goods and services.
Encrypted Network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same

	purposes.
Encryption Key Pair	A public and private key pair issued for the purposes of encrypting and decrypting data.
End Entity	A person, device or application that uses the keys and Certificates created within the PKI for purposes other than the management of the aforementioned keys and Certificates. An End Entity may have the roles of a Subscriber or a Relying Party.
Entity	Any autonomous element within the PKI. This may be a CA, a RA or an End Entity.
Entity CA	A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government.
Employee	An employee is any person employed in or by the State; as well as contractors and other persons who have been authorized to access electronic networks.
FBCA Operational Authority (FPKI OA)	The Federal Public Key Infrastructure Operational Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority.
Federal Information Processing Standards (FIPS)	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Federal Public Key Infrastructure Policy Authority (FPKI PA)	The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-entity PKI interoperability that uses the FBCA.
Firewall	Gateway that limits access between networks in accordance with local security policy. [NS4009]
Governing Body	Authorities that dictate Policy and procedures that may impact the Policy Authority and Operational Authority.

Hardware Token	A hardware device that can hold private keys, digital certificates, or other electronic information that can be used for authentication or authorization. Smartcards and USB tokens are examples of hardware tokens.
High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009]
Inside threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
Integrity	Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination.
Intellectual Property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Issuing CA	In the context of a particular Certificate, the issuing Certificate Authority is the Certificate Authority that signed and issued the Certificate.
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from

ABADSG, "Commercial key escrow service"]

Key Exchange	The process of exchanging public keys in order to establish secure communications.
Key Generation	The process of creating a Private Key and Public Key pair.
Key Generation Material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Key Pair	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the public key, it is computationally infeasible to discover the other key which is called the private key.
Local Registration Authority (LRA)	An entity that is responsible for identification and authentication of Certificate subjects, but that does not sign or issue Certificates (i.e., an LRA is delegated certain tasks on behalf of a RA or CA).
Memorandum of Agreement (MOA)	Agreement between the FPKIPA and an Entity allowing interoperability between the Entity Principal CA and the FBCA.
Mutual Authentication	Occurs when parties at both ends of a communication activity authenticate each other (see authentication).
Naming Authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is registered with an internationally-recognized standards organization.
Operational Authority	An agent of the State PKI CA. The Operational Authority is

(OA)	<p>responsible to the Policy Authority for:</p> <ul style="list-style-type: none"> <li>• Interpreting the Certificate Policies that were selected or defined by the Policy Authority.</li> <li>• Developing a Certification Practice Statement (CPS), in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 2527), to document the CA's compliance with the Certificate Policies and other requirements.</li> <li>• Maintaining the CPS to ensure that it is updated as required.</li> <li>• Operating the Certificate Authority in accordance with the CPS.</li> </ul>
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or is earlier revoked.
Organization	Department, agency, partnership, trust, joint venture or other association.
Out-of-Band	Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online).
Outside Threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
PKIX	A set of IETF Working Group developed technical specifications for PKI components based on X.509 Version 3 Certificates.
Person	A human being (natural person), corporation, limited liability company, or other judicial entity, or a digital device under the control of another person.
PIN	Personal Identification Number. See activation data for definition
PKIX	"Public Key Infrastructure X.509". A set of standards for using X.509 certificates and certificate revocation lists on the



	Internet.
Policy	This Certificate Policy.
Policy Authority (PA)	<p>An agent of the Certificate Authority. The Policy Authority is responsible for:</p> <ul style="list-style-type: none"> <li>• Dispute resolution.</li> <li>• Selecting and/or defining Certificate Policies, in accordance with the Internet X.509 Public Key Infrastructure (PKIX) Certificate Policy and Certification Practice Framework (RFC 2527), for use in the Certificate Authority PKI or organizational enterprise.</li> <li>• Approving of any interoperability agreements with external Certificate Authorities.</li> <li>• Approving practices, which the Certificate Authority must follow by reviewing the Certification Practice Statement to ensure consistency with the Certificate Policies.</li> <li>• Providing Policy direction to the Certificate Authority (CA) and the Operational Authority.</li> </ul>
Principal CA	The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public/Private Key Pair	<p>Two mathematically related keys, having the properties that:</p> <ul style="list-style-type: none"> <li>• One key can be used to encrypt a message that can only be decrypted using the other key.</li> <li>• Even knowing the public key, it is computationally infeasible to discover the private key.</li> </ul>

Registration	The process whereby a user applies to the Certification Authority for a digital certificate and the Certificate Authority (CA) issues a Certificate for that user.
Registration Authority (RA)	An Entity that is responsible for the identification and authentication of Certificate Subscribers before Certificate issuance, but does not actually sign or issue the Certificates (i.e., an RA is delegated certain tasks on behalf of a Certificate Authority (CA)).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key.
Relying Party	A Relying Party is a recipient of a Certificate signed by the State PKI Certificate Authority (CA) who acts in reliance on those Certificates and/or digital signatures verified using that Certificate and who has agreed to be bound by the terms of this CP and the CPS.
Relying Party Agreement	An agreement subscribed to by a recipient of a Certificate signed by the State PKI Certificate Authority (CA) prior to gaining access to any State PKI CA CRL.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	The logical single Repository operated for all Subscribers and Relying Parties on the Network. All Certificates issued by all CAs, and all Certificate Revocation Lists relating thereto, shall be published in the Repository. Also known as a "Directory".
Revocation	To prematurely end the operational period of a Certificate from a specified time forward.
Root CA	The Certificate Authority (CA) that issues Certificates to each CA operating under this Policy.
Security Accreditation Authority	An agent of the CA. Responsible for: <ul style="list-style-type: none"> <li>• Approving the operation of the Certificate Authority (CA) in a particular mode using particular safeguards.</li> <li>• Accepting residual security risks on behalf of the CA domain or enterprise.</li> </ul>
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or

	performing any other cryptographic functions.
Signature Key Pair	A public and private key pair used for the purposes of digitally signing electronic documents and verifying digital signatures.
Software-based Certificate	A digital certificate (and associated private keys) that are created and stored in software – either on a local workstation or on a secure server.
Sponsoring Organization	An organization with which an Authorized Subscriber is affiliated (e.g., as an employee, user of a service, business partner, customer etc.).
Subscriber	An entity that is the subject of a Certificate and which is capable of using, and is authorized to use, the private key, that corresponds to the public key in the Certificate. Responsibilities and obligations of the Subscriber shall be as required by the Certificate Policy.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA).
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA).
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009]
Token	A hardware security device containing an End Entity's Private Key(s) and Public Key Certificate. (see "Hardware Token")
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.

Two-Person Control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009]
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Valid Certificate	A Certificate that (1) a Certificate Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not “valid” until it is both issued by a Certificate Authority (CA) and has been accepted by the Subscriber.
Zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401]

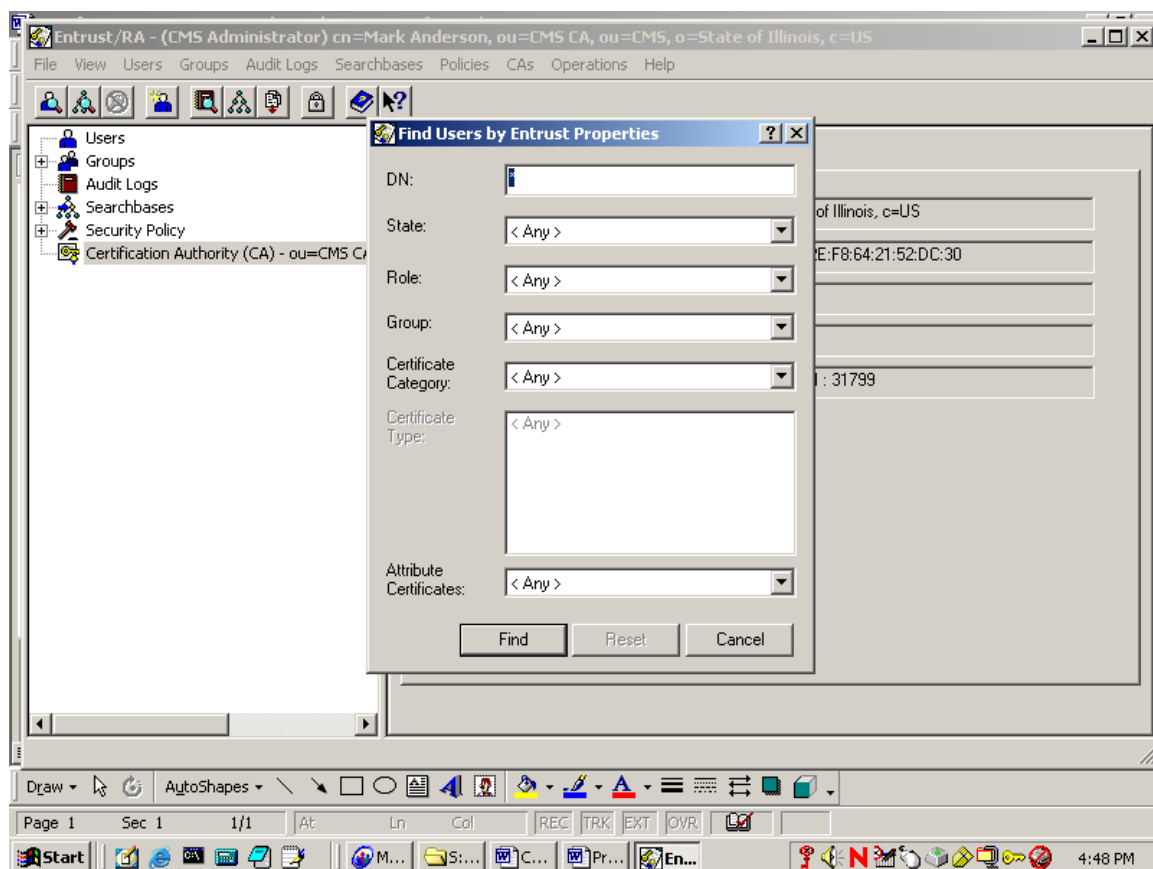
## 13. APPENDIX 1 – CERTIFICATE REVOCATION PROCEDURES

Occasionally, certificates need to be revoked. The rationale behind this decision is detailed in the Certificate Policy and the Certification Practices Statement. All documentation, emails, memos, etc are to be stored in a subdirectory under the S:/Entrust/Revocation Requests folder. A sub-folder should be created for the agency requesting the revocation if one does not exist. You may also create a sub-folder under the agency for a particular revocation request if you desire. The steps for certificate revocation are outlined below:

A Certificate revocation checklist is provided in this appendix: A copy of this checklist should be filled out, printed, and stored with the hardcopy documentation of the revocation request.

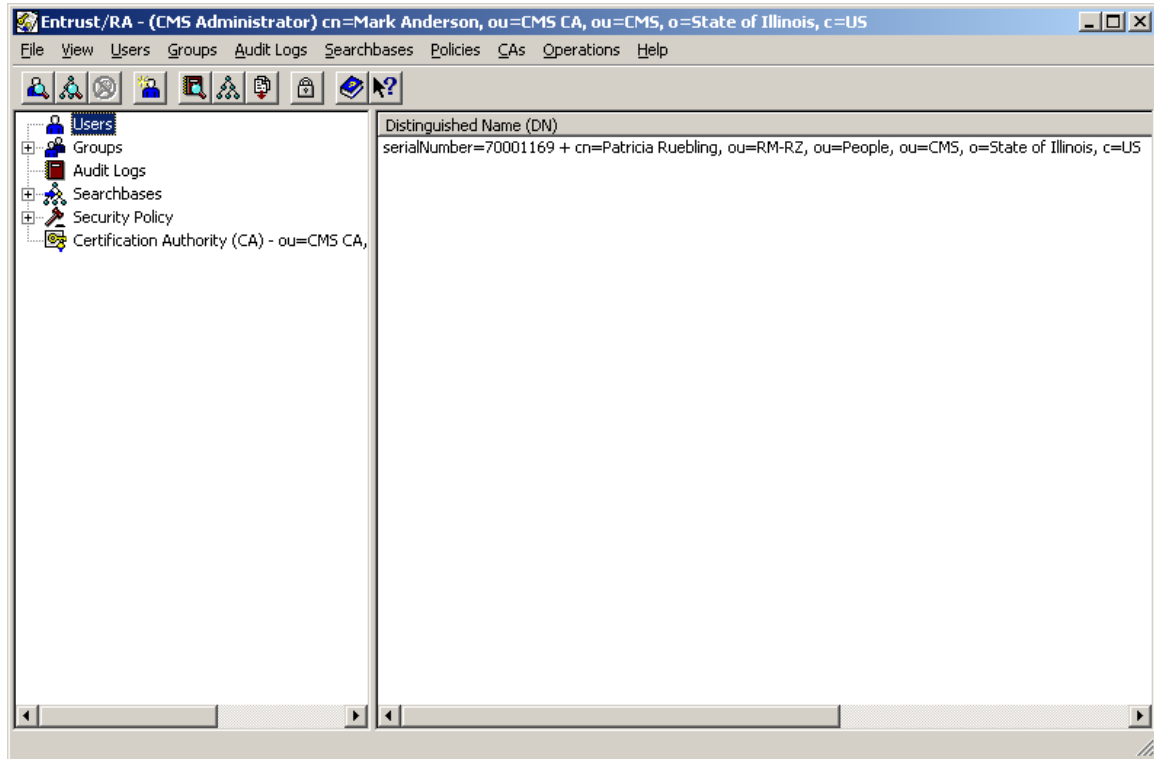
Locate the user to be revoked.

After you have logged in to Entrust RA, locate the desired user. Either click on the “Find user” icon on the far left of the toolbar, or go to “Users – Find – by Entrust Properties” on the main menu.



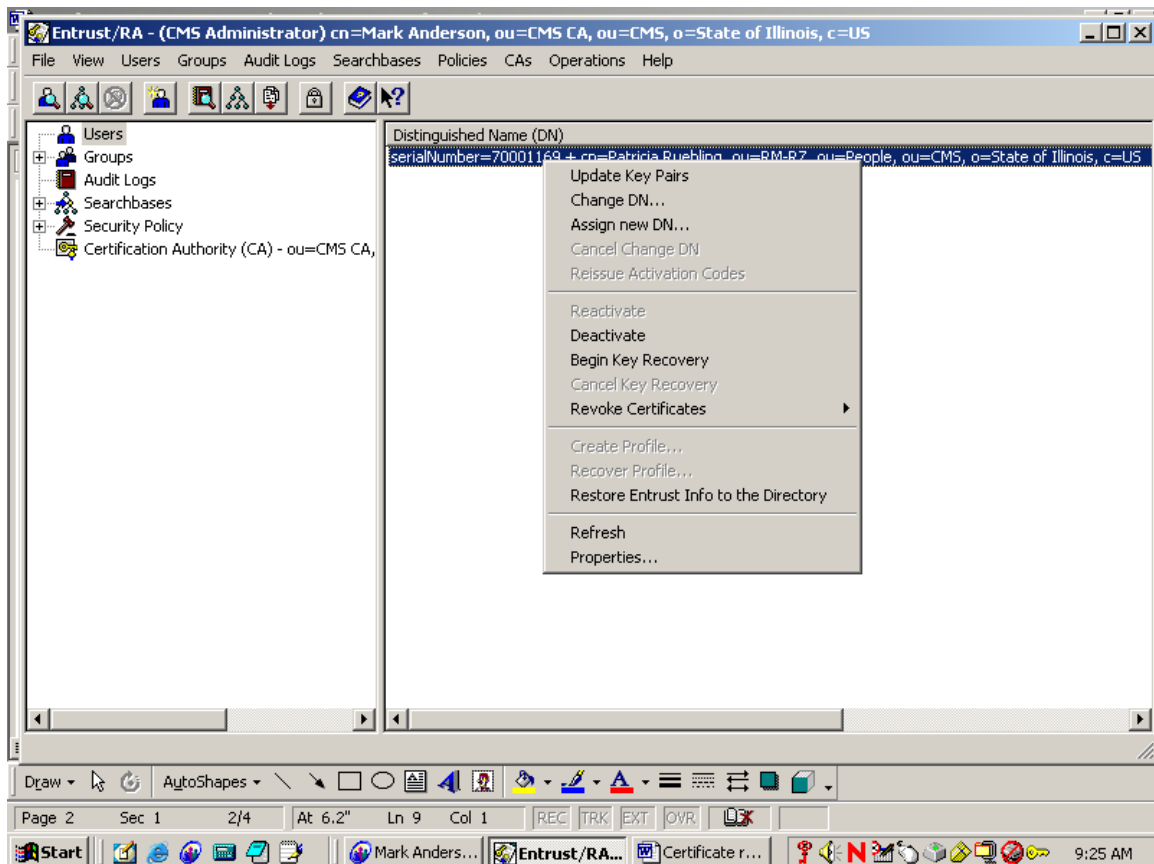
- ✓ Enter the users last name in the “DN” field.
- ✓ Click “Find”.

The users that match the search criteria will be displayed in the right-hand window pane, as follows:

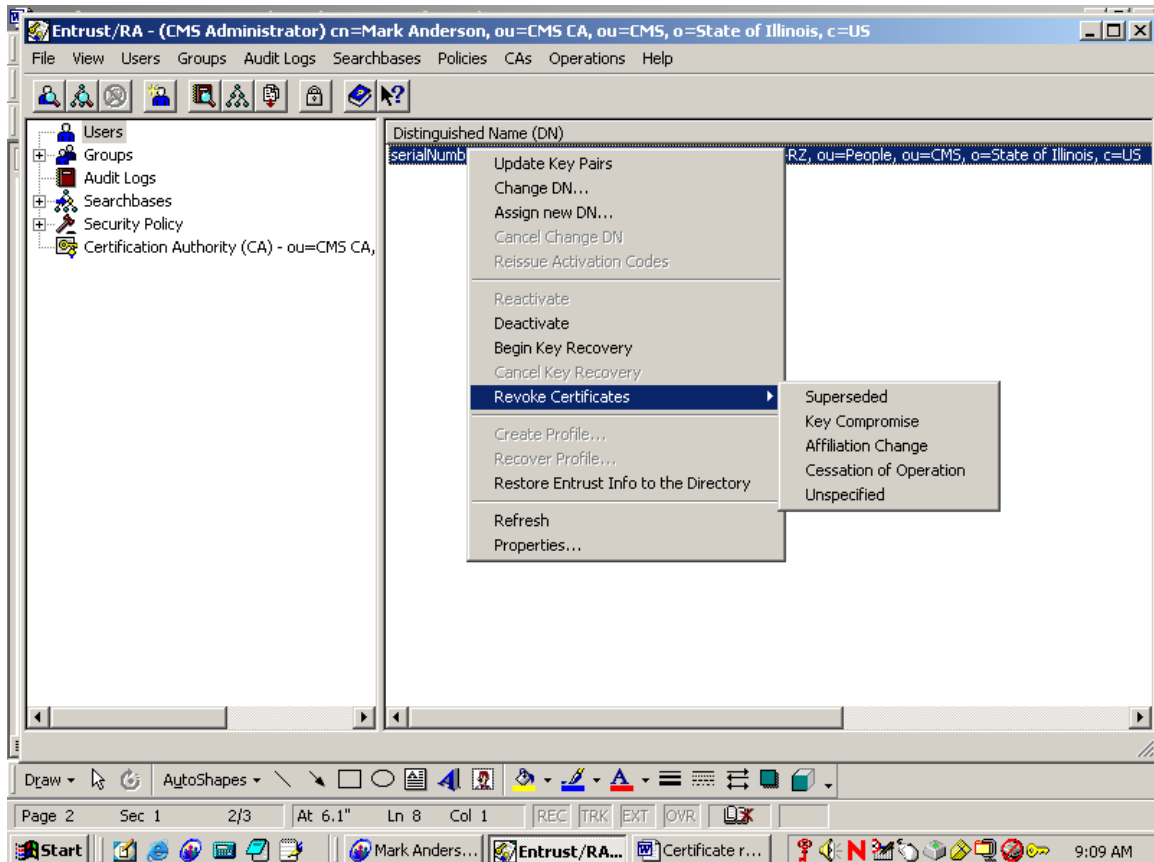


### Revoke the user

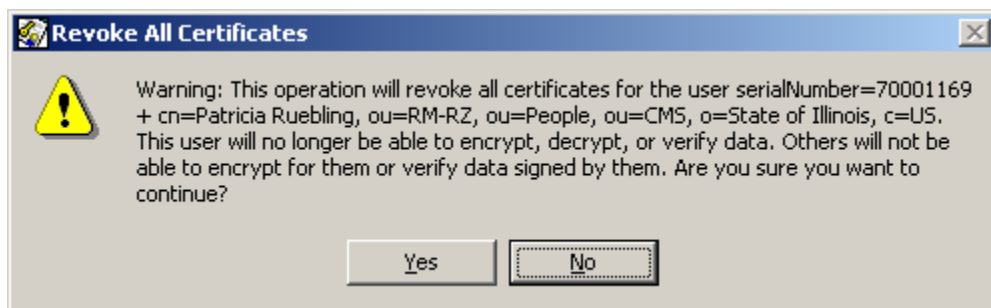
Once the proper certificate has been located, right-click on the entry to display the options menu.



Position your mouse pointer over the “revoke certificates” menu option to display the sub-options.

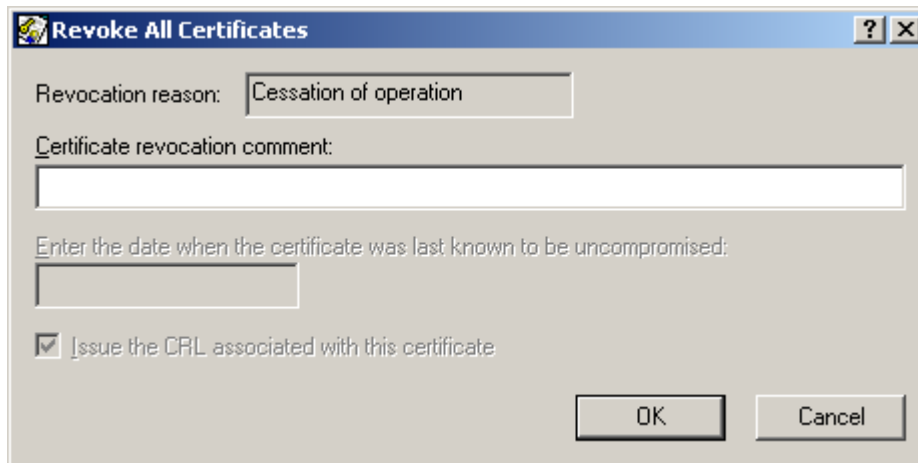


You will need to select and click on the proper reason for the revocation. Upon choosing the correct option, you will see a dialog box resembling the following:

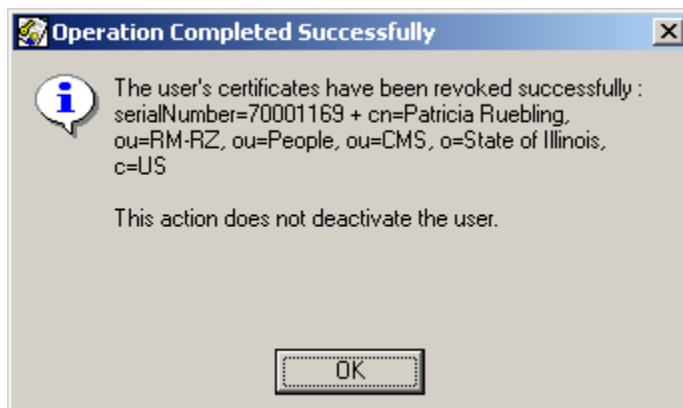


Click "Yes" to continue. You will see the following dialog box:





Enter an appropriate comment in the revocation comment field, and click OK. You will then see the following confirmation dialog box:



## Deactivating the user

Double-click on the user's entry in the right-hand window pane to display the certificate properties.

**User Properties - serialNumber=70001169 + cn=Patricia Ruebling, o=...**

General | Certificate | Encryption Certificates | Verification Certificates | Key Up

User DN: serialNumber=70001169 + cn=Patricia Ruebling, o=...

E-mail (subjectAltName): Pat.ruebling@epa.state.il.us

User role: End User

User group(s):

☒ All groups

Available: default

Assigned:

Add >>

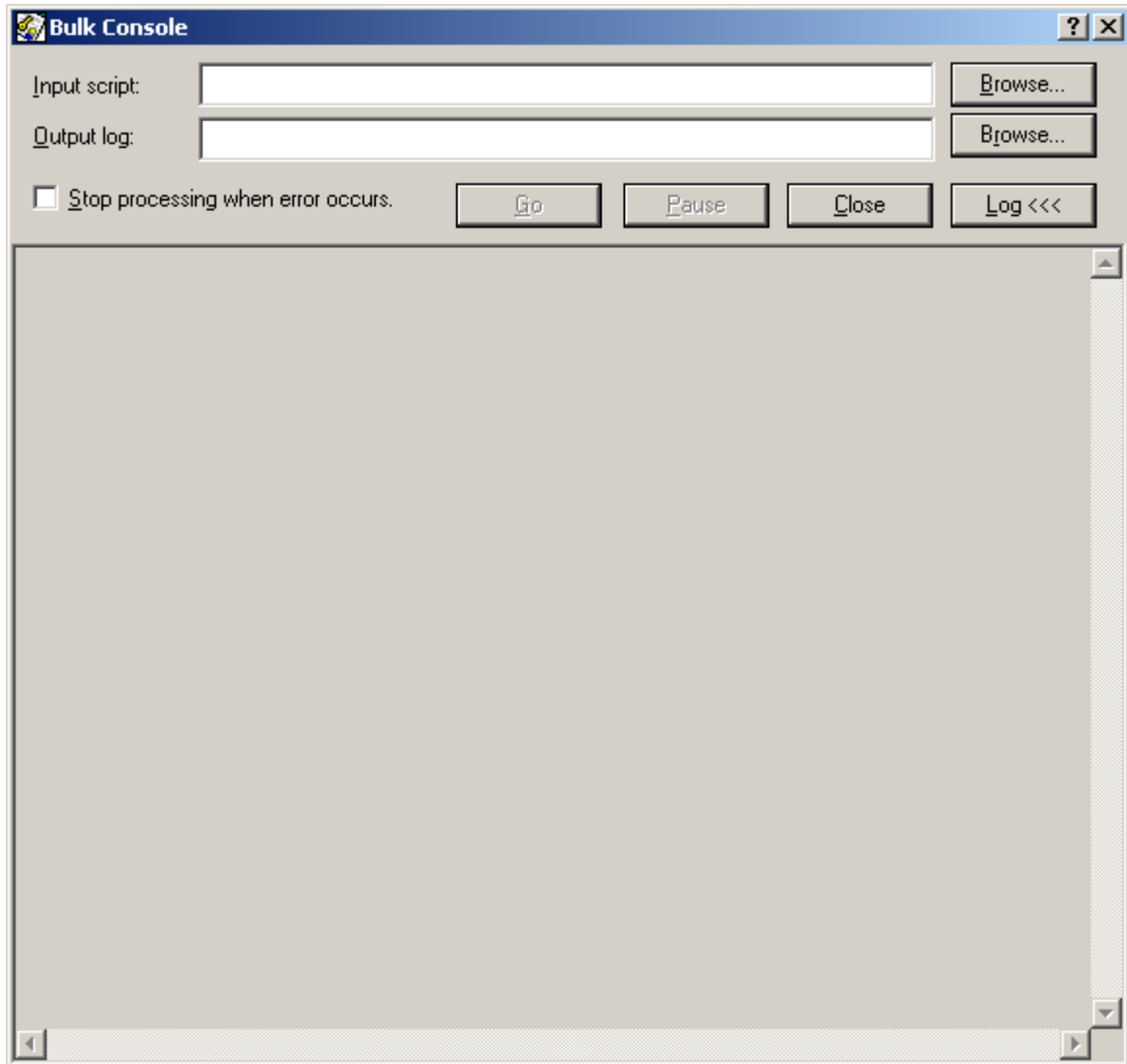
<< Remove

Current state: Active Previous state: Added

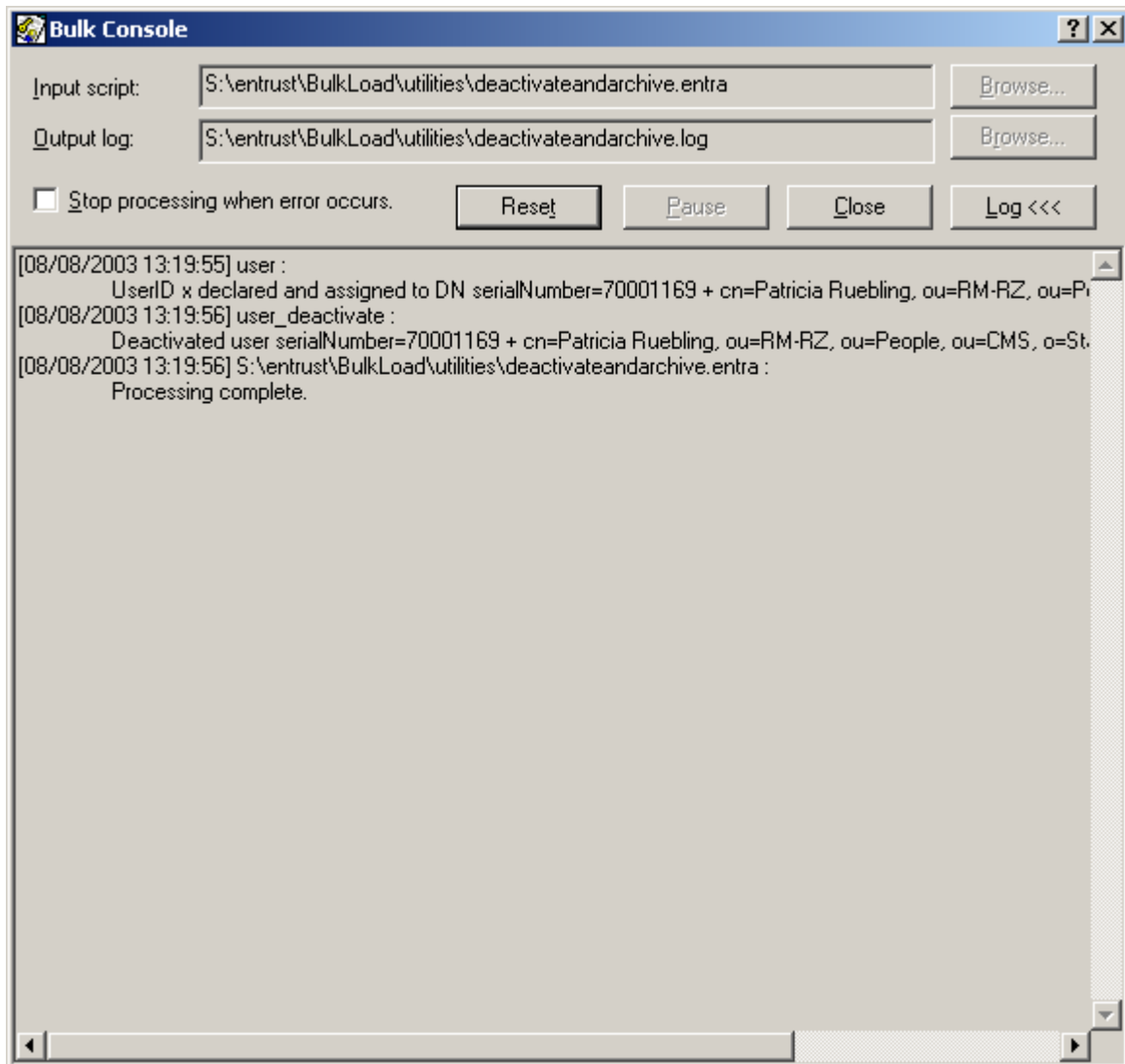
Added: 12/02/2002 1:26:02 Activated: 12/02/2002 1:26:04

OK Undo Apply Cancel

- ✓ Highlight the contents of the DN field and copy it to the windows clipboard (CTRL-C). Click on "Cancel" after doing this.
- ✓ Edit the following file using Notepad:  
[S:\Entrust\Bulkload\utilities\deactivateandarchive.entra.](#)
- ✓ You will see a series of statements in this file. One will begin with "user x", and will contain a distinguished name. Paste the DN that you copied previously into the file where the distinguished name appears. The DN must be enclosed in double-quotes.
- ✓ Make sure that you have a statement following the "user x" statement that reads "user\_deactivate x".
- ✓ Save the file and exit.
- ✓ Go into the bulk load option under Entrust RA:

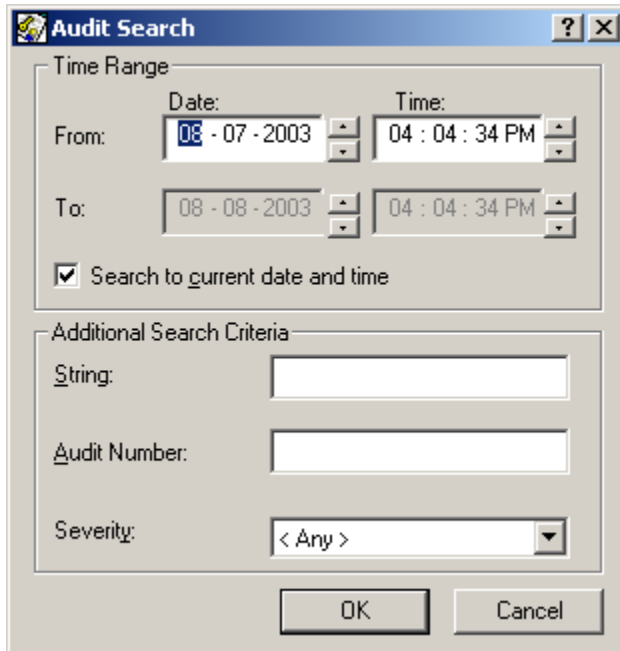


Click on the “browse” button and select the “deactivateandarchive” file that you just edited. Click on the “Go” button to process the file. You will see the following screen:



### Collect the necessary audit logs

When a certificate is revoked and deactivated, entries are placed in the Entrust audit log. In order to verify the revocation, this information should be captured and maintained. To do this, bring up the Entrust RA audit log dialog box:



**Audit Search**

Time Range

From: Date: 08 - 07 - 2003 Time: 04 : 04 : 34 PM

To: 08 - 08 - 2003 04 : 04 : 34 PM

☒ Search to current date and time

Additional Search Criteria

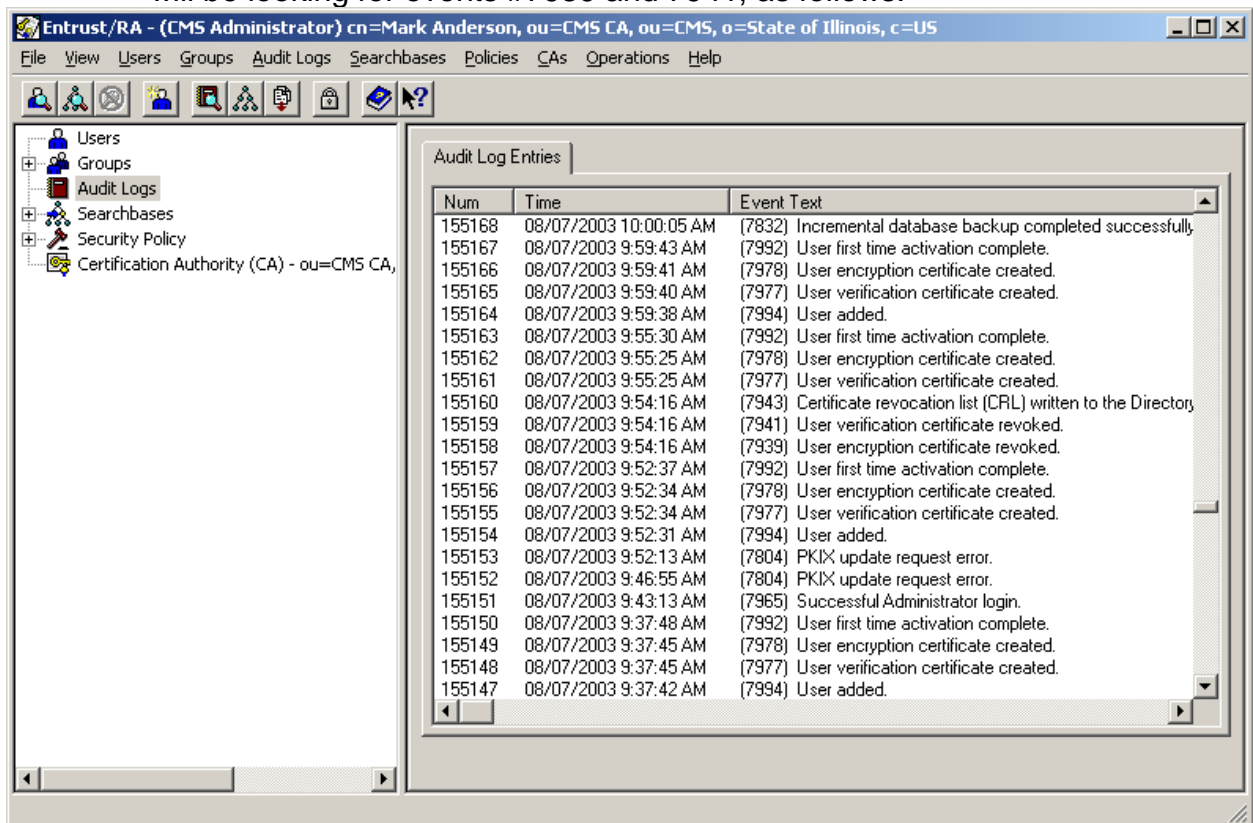
String:

Audit Number:

Severity: < Any >

OK Cancel

- ✓ Enter the date and time the revocation and deactivation took place (in general times; you do not have to put the exact time) and click “OK”. You will see an audit log appear in the right-hand window pane. You will be looking for events #7939 and 7941, as follows:



Entrust/RA - (CMS Administrator) cn=Mark Anderson, ou=CMS CA, ou=CMS, o=State of Illinois, c=US

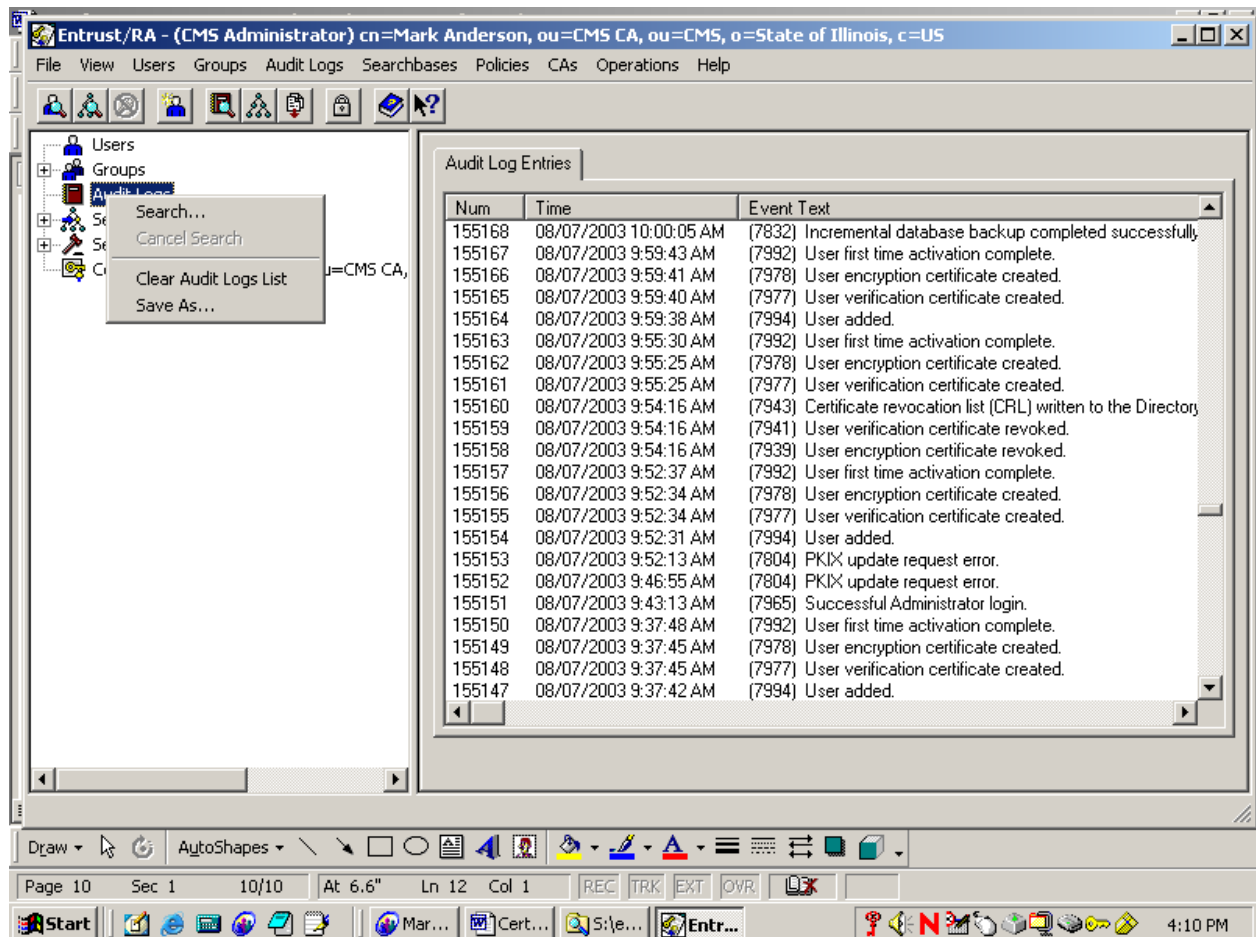
File View Users Groups Audit Logs Searchbases Policies CAs Operations Help

Users Groups Audit Logs Searchbases Security Policy Certification Authority (CA) - ou=CMS CA,

Audit Log Entries

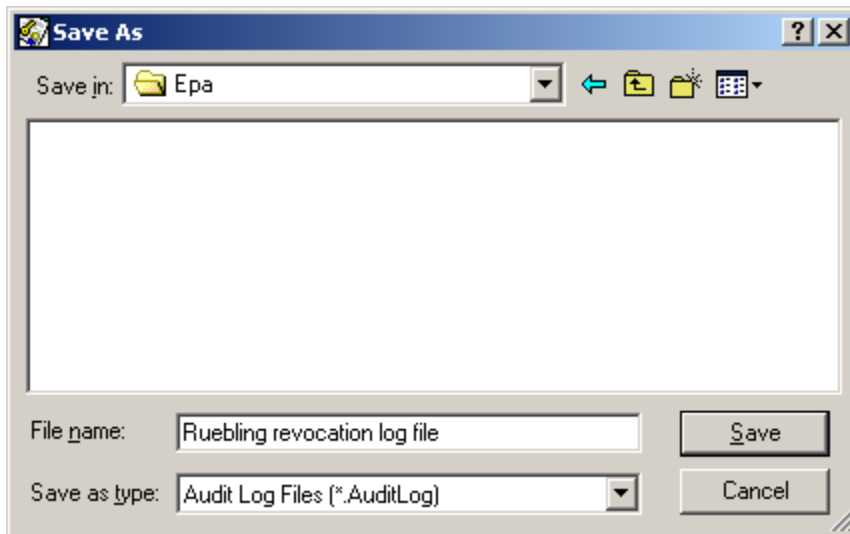
Num	Time	Event Text
155168	08/07/2003 10:00:05 AM	(7832) Incremental database backup completed successfully.
155167	08/07/2003 9:59:43 AM	(7992) User first time activation complete.
155166	08/07/2003 9:59:41 AM	(7978) User encryption certificate created.
155165	08/07/2003 9:59:40 AM	(7977) User verification certificate created.
155164	08/07/2003 9:59:38 AM	(7994) User added.
155163	08/07/2003 9:55:30 AM	(7992) User first time activation complete.
155162	08/07/2003 9:55:25 AM	(7978) User encryption certificate created.
155161	08/07/2003 9:55:25 AM	(7977) User verification certificate created.
155160	08/07/2003 9:54:16 AM	(7943) Certificate revocation list (CRL) written to the Directory.
155159	08/07/2003 9:54:16 AM	(7941) User verification certificate revoked.
155158	08/07/2003 9:54:16 AM	(7939) User encryption certificate revoked.
155157	08/07/2003 9:52:37 AM	(7992) User first time activation complete.
155156	08/07/2003 9:52:34 AM	(7978) User encryption certificate created.
155155	08/07/2003 9:52:34 AM	(7977) User verification certificate created.
155154	08/07/2003 9:52:31 AM	(7994) User added.
155153	08/07/2003 9:52:13 AM	(7804) PKIX update request error.
155152	08/07/2003 9:46:55 AM	(7804) PKIX update request error.
155151	08/07/2003 9:43:13 AM	(7965) Successful Administrator login.
155150	08/07/2003 9:37:48 AM	(7992) User first time activation complete.
155149	08/07/2003 9:37:45 AM	(7978) User encryption certificate created.
155148	08/07/2003 9:37:45 AM	(7977) User verification certificate created.
155147	08/07/2003 9:37:42 AM	(7994) User added.

At this point, right click on the “Audit logs” option on the left-hand side of the screen. You will see an option menu as follows:



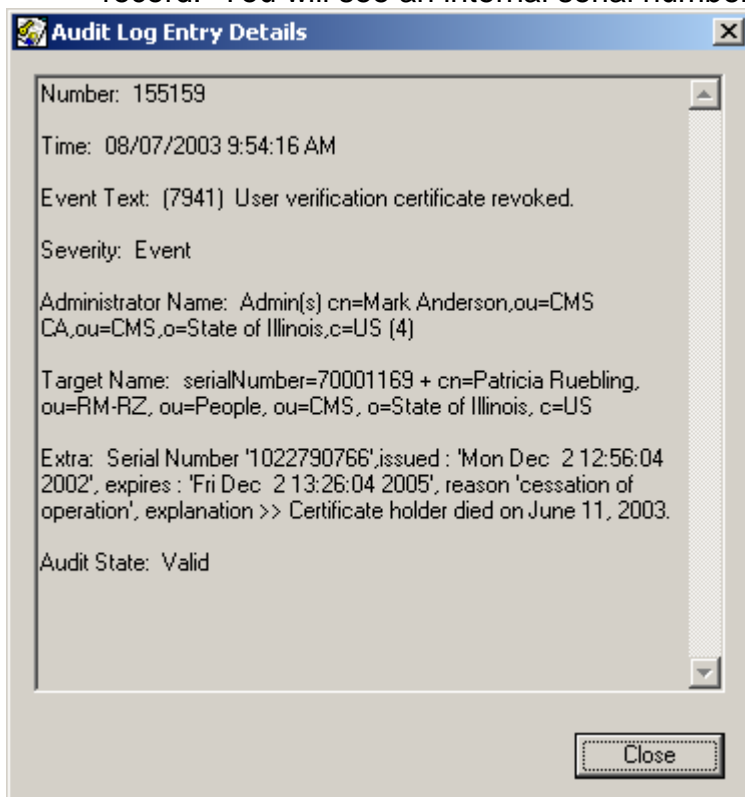
You will be saving this audit log for posterity:

- ✓ Click on the “save as” option to save the audit log to a file. This file should be saved in the folder alluded to in the introductory paragraph.
- ✓ Give the file a meaningful name so it can be identified later. Suggestions would be to include the user’s last name in the file name:



Additionally, you will to gather some serial number information so that we can continue with the next section:

- ✓ Double-Click on the “7941 – User verification certificate revoked” audit record. You will see an internal serial number as follows:



- ✓ Record the internal serial number (in the example above, it is 1022790766). Paste the above dialog box into a file and save it in the defined directory.
- ✓ Do the same for “7939 – User encryption certificate revoked” audit record.
- ✓ Convert the two serial numbers gathered above to hexadecimal. (This is how they are stored in the CRL). You can use the normal calculator that comes with Microsoft Windows or any other means.

Example: The internal serial number gathered above of 1022790766 translates to

3CF68C6E in hexadecimal.

- ✓ Record these numbers. You may enter them in the file created above if you wish.

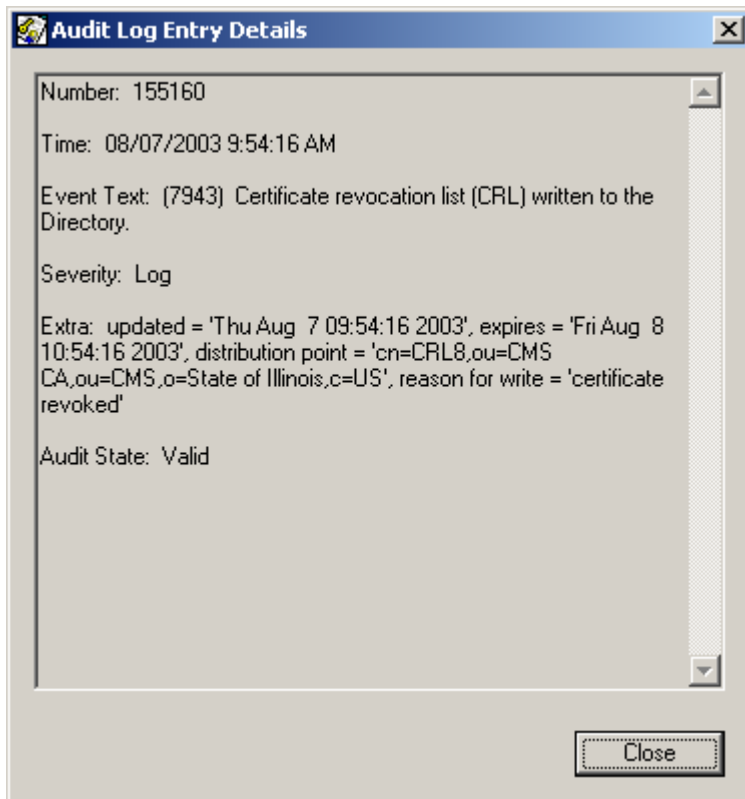
### Obtaining CRL information

When a certificate is revoked, the certificate’s internal serial number is placed in a Certificate Revocation List, or CRL. These files have a distinguished name format similar to the following:

**cn=CRL??,ou=CMS CA, ou=CMS, o=State of Illinois, c=US**, where ?? is a sequential number identifying the certificate revocation list. Whenever we revoke a certificate, we print the content of the CRL so we can prove that the certificate is actually in the CRL. This is done by looking for the 2 internal certificate numbers gathered above in the CRL itself. To do this, you must know which CRL a user’s certificate is pointing to.

- ✓ Check the audit log that you have saved. Directly above the audit records for the certificate revocation is a record indicating a CRL has been written. This message will look similar to this:  
“7943 – Certificate revocation list written to directory”.
- ✓ Double-clicking on this record should display a dialog box similar to the following:





Note that the cn indicates that the CRL name is CRL8, and the reason for writing the CRL is "certificate revoked".

- ✓ Save this dialog box to a file in the prescribed directory.
- ✓ Close out of Entrust RA.

### Displaying serial numbers of revoked certificates in the CRL

The CRL is not a normal file you can browse. You must run a utility called "ldapsearch" to translate the CRL and create a file that can be viewed. This utility can be found in the following folder: **S:\Entrust\PKI Procedures\CRL information** in a file named **Export CertificateRevocationLists.bat**. The contents of this file are similar to the following:

Echo off

```
ldapsearch -h 10.201.80.16 -p 389 -V 3 -b "cn=CRL13,ou=CMS CA, ou=CMS,
o=State of
Illinois, c=US" -t objectclass=* CertificateRevocationList > c:\temp\ldapsearch.out
```

echo

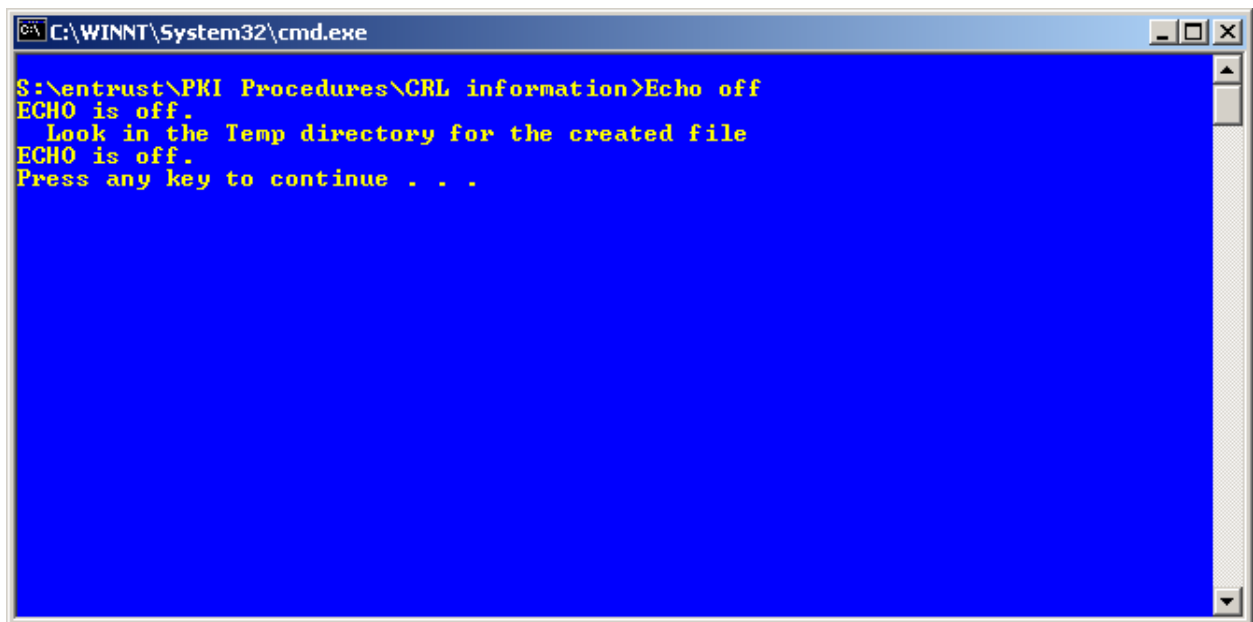
echo Look in the Temp directory for the created file

echo

pause

Echo on

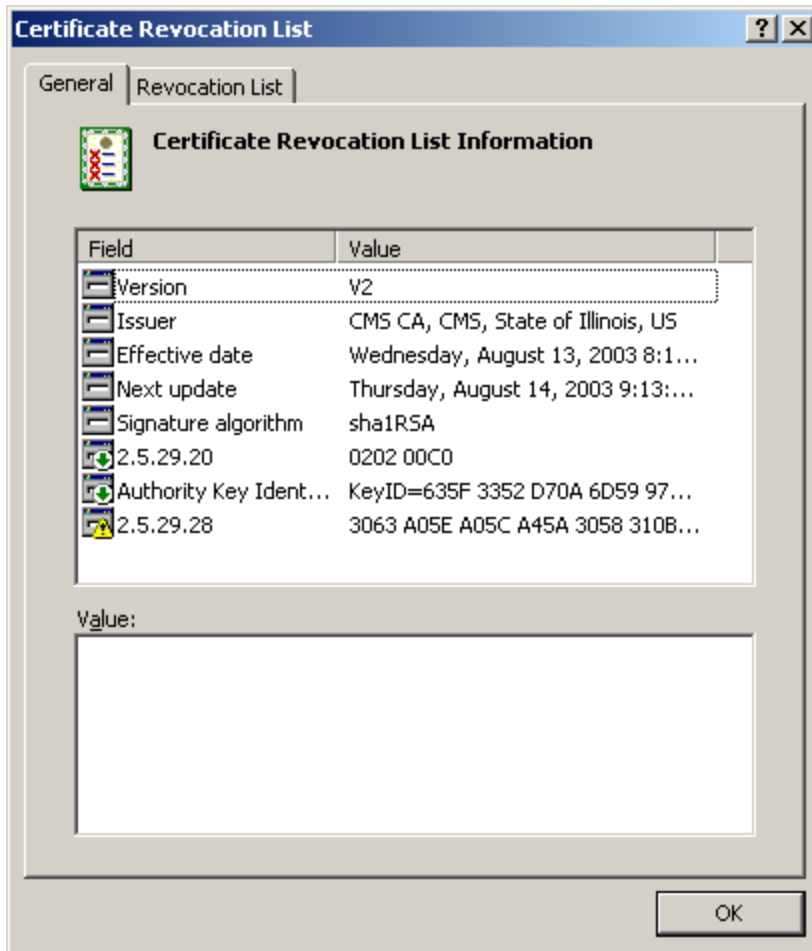
- ✓ Edit this file (using notepad) and change the CRL number on the second line to the CRL you want to display (in this case, 8).
- ✓ Save the file.
- ✓ Double-click on the file to execute it. You will see a screen similar to the following:



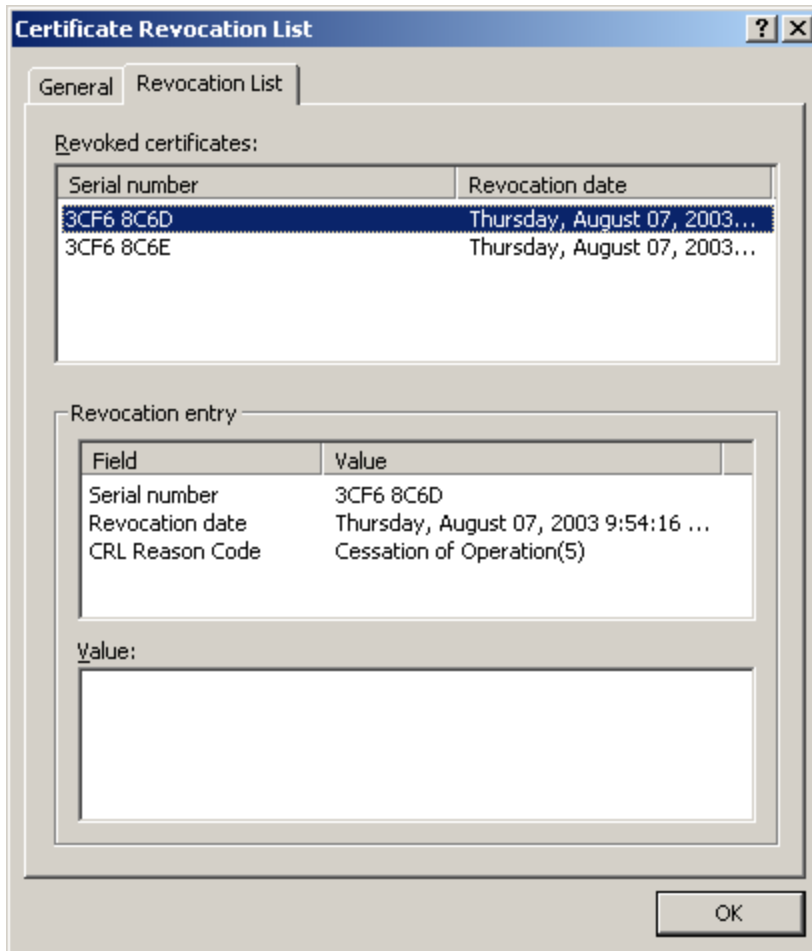
A screenshot of a Windows command prompt window titled "C:\WINNT\System32\cmd.exe". The window has a blue background and a white border. The text displayed in the window is as follows:

```
S:\entrust\PKI Procedures\CRL information>Echo off
ECHO is off.
Look in the Temp directory for the created file
ECHO is off.
Press any key to continue . . .
```

- ✓ Using Windows explorer, look in your current directory for a file resembling the following: **ldapsearch-certificateRevocationList;binary-a02128**
- ✓ Rename this file to something like CRL8.crl.
- ✓ Double-click on this file to open it. You will see something like the following:



- ✓ Click on the “Revocation List” tab to display the revoked certificates. It will resemble the following:



The two certificate serial numbers (in hex) should appear in the “Revoked certificates”. Make a screen print of this dialog box and save it in the prescribed directory.

### **Print and file the information**

The final step in certificate revocation is to print and file all of the documents that you have collected and file them in the “Revoked Certificates” folder which is stored in the locked file cabinet in the PKI room. This is necessary for audit purposes.

**Below is the checklist that must be followed when performing a certificate revocation.**

1. \_\_\_\_ Receive notification from LRA, certificate user, or Policy Authority, that requests the certificate be revoked. This correspondence must be hard copy signed or sent through e-mail digitally signed.
2. \_\_\_\_ CA prints off e-mail and corresponding digital signature for hard copy proof or retains hard copy request from user or Policy Authority.
3. \_\_\_\_ CA revokes the digital certificate in question and states in the revocation, the nature of the revocation and origin of request.
4. \_\_\_\_ CA deactivates and archives the certificate that has been revoked.
5. \_\_\_\_ CA pulls log files to show the actions that were performed and saves file in the revocation folder.
6. \_\_\_\_ The CA must verify that the certificate revocation lists have been updated with the serial numbers of the certificate that was revoked and print hard copy.
7. \_\_\_\_ CA prints the log file page that shows the actions performed and stores it with the other documents collected including this one in the revocation binder.
8. \_\_\_\_ CA completes this form and signs below and stores all hard copy documents in the revocation binder organized by year.

Circumstances that led to revocation:

---

---

---

---

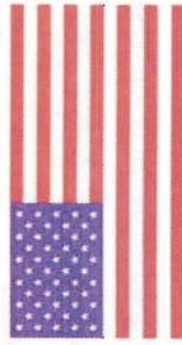
---

---

Signed: \_\_\_\_\_ Date: \_\_/\_\_/\_\_

## **14. APPENDIX 2 – FIPS 140-1 VALIDATION CERTIFICATE**

# FIPS 140-1 Validation Certificate



The National Institute of Standards  
and Technology of the United States  
of America



The Communications Security  
Establishment of the Government  
of Canada

Certificate No. 214

The National Institute of Standards and Technology, as the United States FIPS 140-1 Cryptographic Module Validation Authority; and the Communications Security Establishment, as the Canadian FIPS 140-1 Cryptographic Module Validation Authority; hereby validate the FIPS 140-1 testing results of the Cryptographic Module identified as:

**Luna® CA3, by Chrysalis-ITS Incorporated**  
(When operated in FIPS mode)

In accordance with the Derived Test Requirements for FIPS 140-1, *Security Requirements for Cryptographic Modules*. FIPS 140-1 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *Sensitive But Unclassified Information* (United States) or *Designated Information* (Canada) within computer and communications systems (including voice systems).

Products which use the above identified cryptographic module may be labeled as complying with the requirements of FIPS 140-1 so long as the product, throughout its life cycle, continues to use the validated version of the cryptographic module as specified in this certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.



and tested by the Cryptographic Module Testing accredited laboratory: DOMUS IT Security Laboratory, NVLAP LAB CODE 200017-0  
is as follows:

Cryptographic Module Design:	Level 3	Module Interfaces:	Level 3
Roles and Services:	Level 3	Finite State Machine Model:	Level 3
Physical Security: (Multi-chip Standalone)	Level 3	Software Security:	Level 3
EMI / EMC:	Level 3	Self Tests:	Level 3
Key Management:	Level 3		

Operating System Security Level N/A is met when used in the following configuration(s): N/A

The following FIPS approved Cryptographic Algorithms are used: DES (Cert. #32); Triple-DES (Cert. #73); DSA (Cert. #13) SHA-1 (Cert. #64); DES-MAC; Triple-DES MAC; RSA (ANSI X9.31, vendor affirmed)

The Cryptographic module also contains the following non-FIPS approved algorithms: RC2; RC4; RC5; CAST; CAST 3; CAST 5; CAST MAC; CAST 3 MAC; CAST 5 MAC; MD2; MD5; Diffie-Hellman (key agreement); RSA (Encryption and Decryption)

End user queries concerning the non-FIPS approved algorithms may be directed to their respective Cryptographic Module Validation Authority.

**Overall Level Achieved: 3**

Signed on behalf of the Government of the United States

Signature: [Signature]

Dated: 2 May 2002

Chief, Computer Security Division  
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: [Signature]

Dated: 29 April 2002

Director, Information Protection Group  
The Communications Security Establishment